RECHT: JOURNAL OF LEGAL STUDIES
Volume 01 No.1, Maret 2026
e- ISSN No. xxxx-xxxx
Lembaga Penelitian dan Kajian Hukum, Fakultas Hukum Universitas Trisakti
This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

Constitutional Limits on State Digital Surveillance in Indonesia: A Proportionality Test of Privacy and Due Process

Arditya Prayogi[a], Muhammad Sobri Maulana[b], Dwitia Pratiwi[c]

[a]*UIN K.H. Abdurrahman Wahid Pekalongan*
arditya.prayogi@uingusdur.ac.id
[b]*RSAU Esnawan Antariksa Jakarta*
muhammadsobrimaulana31@gmail.com
[c]*RSAU Esnawan Antariksa Jakarta*
pdwitia@gmail.com

Abstract

This paper examines the constitutional limits on state digital surveillance in Indonesia through the lens of the proportionality test and due process. It asks how Indonesia's constitutional framework, particularly the 1945 Constitution (UUD 1945), constrains digital surveillance and whether existing laws and practices respect privacy, freedom of communication and fair trial rights. Drawing on doctrinal legal research and comparative constitutionalism, the study develops a conceptual framework of digital surveillance, privacy and due process and applies a four-step proportionality test—legality, legitimate aim, necessity and proportionality stricto sensu—to various forms of state surveillance, including targeted interception, mass data collection and platform-based monitoring. It finds that Indonesia's legal landscape is fragmented and often lacking clear statutory authority for surveillance; regulations such as Ministerial Regulation No. 5 of 2020 grant authorities "direct access" to user datawhile investigative agencies have acquired powerful spyware and IMSI-catcher technologies. Yet the Personal Data Protection Law of 2022 promises stronger safeguards and rights of consent. The analysis argues that any digital surveillance must satisfy a strict proportionality test and be accompanied by due process safeguards such as judicial authorization, specificity, minimization, time limits and effective oversight. The paper offers normative recommendations for reforming Indonesia's legal framework to balance national security with constitutional rights, and concludes that robust due process mechanisms are essential to prevent privacy erosion in the digital age.

Keywords: *Digital surveillance; Proportionality test; Privacy; Due process; Indonesia; Constitutional law.*

I. Introduction

The proliferation of digital technologies has reshaped how states monitor, collect and analyse information about individuals. In Indonesia, the transition from authoritarian rule in 1998 to a democratic constitutional order has been accompanied by rapid internet penetration and the rise of data-driven policing and intelligence practices. Government agencies have reportedly purchased spyware systems such as FinFisher and Circles to intercept communications and extract data from devices, and they have deployed applications like PeduliLindungi now rebranded as SatuSehat to collect location and health data during the COVID-19 pandemic. At the same time, regulatory instruments such as Governmental Regulation No. 71 of 2019, the Electronic Information and Transactions (ITE) Law and Ministerial Regulation No. 5 of 2020

(MR 5/2020) have broadened state access to personal data by requiring electronic system providers to grant authorities direct system access and comply with data retention obligations. These developments raise pressing questions: What are the constitutional boundaries of digital surveillance in Indonesia? How can privacy and due process rights be protected in an era of mass data collection and algorithmic profiling? And what legal reforms are needed to align Indonesian practices with international human rights standards?

This paper seeks to answer these questions by examining the constitutional limits on state digital surveillance through the lens of the proportionality test and due process guarantees. It builds a normative framework that situates digital surveillance within the broader context of constitutional rights, including the right to privacy, freedom of expression, freedom of communication and the right to a fair trial. Under Article 28G of the UUD 1945, every person has the right to protection of themselves, their family, honour, dignity and property, and under Article 28F individuals have the right to communicate and obtain information through any available channel. Article 28D guarantees due process and legal certainty. The Constitution also permits restrictions on rights where prescribed by law and necessary to uphold public order and morality, national security or the rights of others. The challenge is to ensure that surveillance measures comply with these limitations without eroding core liberties.

The paper proceeds in eight parts. The first section outlines the conceptual framework of digital surveillance, privacy and due process. The second analyses the Indonesian constitutional and legal landscape, highlighting statutory provisions, constitutional jurisprudence and the fragmentation of authority across law enforcement and intelligence agencies. The third introduces the proportionality test as an analytical tool and adds a procedural dimension to account for due process safeguards. The fourth applies the proportionality test to three normative scenarios—targeted surveillance, bulk/untargeted surveillance and platform-based monitoring and automated profiling—evaluating how each form of surveillance measures up against constitutional standards. The fifth discusses due process requirements and remedies, while the sixth offers normative reform proposals, drawing on comparative experiences from jurisdictions such as Germany and the European Court of Human Rights (ECHR). A concise policy implications section distils the findings into actionable recommendations for policymakers and civil society. The paper concludes by summarizing the contributions and proposing an agenda for future research

II. Conceptual Framework: Digital Surveillance & Constitutional Rights

Digital surveillance refers to the collection, analysis and use of electronic data to monitor individuals or groups. In the context of law enforcement and national security, surveillance tools include interception (wiretapping), metadata collection, international mobile subscriber identity (IMSI) catchers that emulate cell towers to capture mobile signals, monitoring platforms that aggregate social media posts, data retention schemes, lawful access demands on service providers, and automated profiling that employs algorithms to infer behaviour. These practices are distinguished from targeted investigation by their scale and reliance on digital infrastructures.

Privacy is not an absolute concept but a bundle of protections against arbitrary or unlawful

interference. It encompasses the right to control personal information, maintain autonomy over communications and be free from intrusive observation. The United Nations International Covenant on Civil and Political Rights (ICCPR) recognises privacy under Article 17 and has interpreted it in General Comment No. 16 to require that any interference be prescribed by law, pursue a legitimate aim and be necessary and proportionate. Privacy also interacts with freedom of expression and association: surveillance can chill speech, deter dissent and undermine democratic participation. The 'chilling effect' describes how awareness of surveillance leads individuals to self-censor, thereby weakening public discourse and accountability.

Due process, or procedural fairness, ensures that individuals are afforded fair and transparent procedures before the state interferes with their rights. Core elements include prior judicial authorization, notice (where compatible with legitimate purposes), the opportunity to challenge surveillance orders, independent oversight, accountability mechanisms and effective remedies. Without due process, surveillance may operate in secrecy and evade scrutiny, resulting in abuses such as political spying, discrimination and denial of fair trial rights.

In constitutional theory, the rule of law demands that state power be exercised in accordance with clear, accessible and predictable laws. Digital surveillance implicates the rule of law because it often relies on executive discretion, secret decrees or vague authorizations. For surveillance to be compatible with constitutionalism, it must satisfy the principle of legality (be based on law), serve a legitimate aim (such as national security or crime prevention), be necessary (the least intrusive means to achieve the aim) and be proportionate stricto sensu (balancing benefits against rights costs). This four-step proportionality test, pioneered in German constitutional jurisprudence and adopted by the European Court of Human Rights, will serve as the primary analytical tool in this paper. We add a fifth dimension—procedural proportionality—to ensure that due process safeguards are integrated throughout. Together, these concepts provide a normative framework for evaluating digital surveillance in Indonesia.

III. Indonesian Constitutional & Legal Landscape

The Indonesian Constitution (UUD 1945) contains several provisions that underpin privacy, communication and due process rights. Article 28G(1) protects the right of individuals to protect themselves, their family, honour, dignity and property; it has been interpreted as encompassing personal data and privacy. Article 28F guarantees the right to communicate and obtain information using all available means, subject to restrictions set by law. Article 28D(1) ensures the right to equal treatment under the law and legal certainty, including fair process before deprivation of liberty or property. Article 28J allows limitations on rights to respect the rights of others and to meet demands of justice, morality and public order within democratic society. The Constitutional Court has emphasised that restrictions must be based on law, proportional and not undermine the essence of the right. However, the Court's jurisprudence on surveillance is limited, reflecting the novelty of digital technologies and the political sensitivity of security measures.

Indonesia has enacted various laws affecting digital surveillance. The ITE Law criminalises defamation, hate speech and other online offences, and enables law enforcement to request data from service providers. Governmental Regulation No. 71 of 2019 implements data localization

and requires providers of public services to maintain servers within Indonesia. Ministerial Regulation No. 5 of 2020 obliges private electronic system operators to register, remove content upon government request and provide 'direct access' to user data for law enforcement. This sweeping regulation was justified as ensuring content moderation and combating criminal activity but drew criticism for its potential to enable mass surveillance and censorship. In practice, authorities temporarily blocked websites and services that failed to comply and used the regulation to request personal data and location information.

The Personal Data Protection (PDP) Law, signed in October 2022, establishes a general framework for personal data rights, including consent, purpose limitation, data minimization and retention limits. It provides for criminal penalties for unlawful collection and misuse of data and mandates the creation of a data protection authority. Yet concerns remain that the authority is housed under the executive branch and may lack independence and enforcement power. Many sector-specific laws—such as the Telecommunications Law, Law on State Intelligence, Banking Law and Population Administration Law—contain provisions for data interception, retention and sharing, often without judicial oversight. For instance, a 2000 government regulation requires telecommunications providers to retain call records for at least three months【37312076925809 5†L1093-L1100】. The result is a fragmented legal landscape where multiple agencies—including the police, Corruption Eradication Commission (KPK), intelligence services and military—conduct surveillance under overlapping mandates.

Judicial authorization for wiretapping has been inconsistently applied. The KPK must obtain permission from a court, whereas other agencies rely on ministerial or internal authorizations. In practice, secretive instructions and broad definitions of national security allow for surveillance that escapes external review. Civil society organizations have documented cases of targeted and bulk interception, including the use of spyware and IMSI catchers to monitor activists and minority groups. Transparency is limited: there is no unified reporting requirement for the number of surveillance orders issued, the categories of data collected, or the outcomes of investigations. Consequently, individuals rarely receive notice that they were surveilled, hindering their ability to seek remedies.

IV. Proportionality Test as Analytical Tool

The proportionality test is a methodological device used by courts to balance conflicting rights and interests. Originating in German constitutional law and refined by the European Court of Human Rights and other jurisdictions, the test comprises four main steps: 1) Legality: The interference must have a basis in law, and the law must be clear, accessible and foreseeable. 2) Legitimate aim: The state must pursue a legitimate objective such as national security, public safety or the rights of others. 3) Necessity: The measure must be necessary to achieve the aim—meaning there are no less intrusive but equally effective alternatives. 4) Proportionality stricto sensu: A balancing exercise weighing the benefits of the measure against the harm to the right. A measure fails this step if the rights impairment outweighs the intended benefits.

Legality requires a detailed legislative framework that specifies who can authorize surveillance, under what conditions and subject to what limits. Vague or secretive regulations

cannot justify intrusive monitoring. Legitimate aims must be concrete and compelling; generic references to national security are insufficient without articulated threats. Necessity demands that authorities exhaust less intrusive methods—such as targeted investigation or data minimization—before resorting to comprehensive surveillance. Proportionality stricto sensu asks whether the intrusion is commensurate with the aim, taking into account the severity of rights restrictions, the probability of harm prevented and the availability of safeguards.

Many scholars argue that the proportionality test should incorporate procedural guarantees. Due process safeguards ensure that the test is not merely formal but substantively effective. We therefore propose a fifth step—'procedural proportionality'—which includes: judicial authorization by an independent and competent authority; specificity of surveillance orders (targeted identifiers, time limits and minimization techniques); transparency mechanisms such as public reporting and individual notice; independent oversight bodies with audit powers; and accessible remedies for affected individuals. This procedural layer aligns the proportionality test with international human rights standards and provides a template for evaluating Indonesia's surveillance framework.

V. Application: Proportionality Analysis of State Digital Surveillance in Indonesia

To illustrate how the proportionality test applies to Indonesia's surveillance practices, this section considers three normative scenarios: targeted surveillance, bulk or untargeted surveillance and platform-based monitoring and automated profiling. Each scenario is examined through the four substantive steps of legality, legitimate aim, necessity and proportionality stricto sensu, followed by a discussion of procedural proportionality.

1. Targeted Surveillance

Targeted surveillance involves intercepting the communications of a specific individual or group based on reasonable suspicion of wrongdoing. In Indonesia, wiretapping in corruption cases requires judicial authorization when conducted by the KPK, but other law enforcement agencies can obtain ministerial approval without court oversight. Legality is therefore inconsistent: the absence of a comprehensive interception statute means that authorization procedures vary across institutions. Legitimate aims—such as investigating terrorism, corruption or serious crime—are clear, but they must be narrowly construed. Necessity requires that investigative authorities show that less intrusive techniques (such as physical surveillance, subpoenas or targeted metadata requests) would be insufficient. Proportionality stricto sensu weighs the severity of privacy intrusion against the anticipated benefit of solving a serious crime. If targeted surveillance is subject to strict judicial oversight, specific time limits and minimization requirements, the balance may favour its use. Procedural proportionality demands independent courts to issue warrants, detailed orders specifying the target and duration, logging and auditing of all access, and ex post notice to individuals once the investigation no longer risks being compromised. Indonesia's current practice falls short of these safeguards, particularly when agencies other than the KPK engage in interception without judicial review.

2. Bulk or Untargeted Surveillance

Bulk surveillance refers to indiscriminate collection of communications or metadata across large populations. Examples include requiring service providers to store all traffic data for future access or using IMSI catchers to sweep mobile signals in a geographic area. Under MR 5/2020, authorities can obtain 'direct access' to servers and user data from electronic system operators, which may facilitate bulk data collection. Legality is questionable because neither MR 5/2020 nor related statutes clearly define the scope and limits of such access. Legitimate aims, such as preventing terrorism or cybercrime, cannot justify indiscriminate collection without individualized suspicion. Necessity fails when bulk collection yields large amounts of irrelevant data and less intrusive methods exist, such as targeted preservation orders. Proportionality stricto sensu reveals that the harms—including chilling effect on free expression, potential abuse of data, discrimination against minority groups and erosion of trust—outweigh the uncertain security benefits. Procedural proportionality would require prior judicial approval for any mass collection, strict retention limits, independent oversight, statistical reporting on the efficacy of bulk surveillance, and robust encryption to prevent misuse. Indonesia currently lacks these safeguards, rendering bulk surveillance incompatible with constitutional standards. Civil society reports and the Freedom House assessment note that authorities have used spyware, IMSI catchers and other technologies to monitor activists and minorities, underscoring the risk of abuse.

3. Platform-based Monitoring & Automated Profiling

Platform-based monitoring involves systematic collection and analysis of data from social media and other online platforms. Automated profiling uses algorithms and machine learning to draw inferences about individuals' behaviour, preferences or risk of criminality. In Indonesia, MR 5/2020 requires platforms to remove content and provide access to user data, enabling authorities to monitor speech and profile users. Legality concerns arise because no comprehensive law regulates algorithmic profiling or content monitoring; regulations are often issued by the executive branch without parliamentary debate. Legitimate aims such as combating disinformation or hate speech must be balanced against the right to free expression and non-discrimination. Necessity is dubious given that proportionate responses—like targeted takedown requests or user-empowered content reporting—can address harmful content without sweeping surveillance. Proportionality stricto sensu demands scrutiny of algorithmic biases, error rates and the risk of discriminatory outcomes. Procedural proportionality requires transparency about algorithms, impact assessments, avenues for contesting decisions, regular audits by independent bodies and public reporting. Indonesia's current framework does not mandate algorithmic transparency or provide meaningful redress for individuals adversely affected by automated profiling. Combined with criminal provisions in the ITE Law and the new Criminal Code that criminalize false information and insults, platform-based monitoring may chill legitimate speech

VI. Due Process Requirements & Remedies

Effective due process safeguards are essential to ensure that digital surveillance respects constitutional rights. First, authorization should rest with an independent and competent authority—preferably a court—rather than the executive. Judges must have access to sufficient information to evaluate necessity and proportionality, and their decisions should be subject to appeal or review. Second, surveillance orders must be specific: they should identify the

individual or entity to be monitored, specify the data sought, set clear time limits and incorporate minimization techniques to exclude irrelevant information. General or open-ended authorizations enable fishing expeditions and are incompatible with due process. Third, chain-of-custody rules must govern the handling of collected data to ensure its integrity, prevent tampering and preserve its admissibility in court. Records of access should be logged and subject to audit.

Fourth, transparency and disclosure play a pivotal role. While real-time notice may jeopardize investigations, delayed notice should be provided once the risk subsides. Public reporting on the number of surveillance orders issued, the categories of offences investigated and the outcomes should be mandated. Fifth, individuals must have effective remedies: they should be able to challenge surveillance orders, seek exclusion of unlawfully obtained evidence and claim compensation for violations. Indonesian courts have recognized exclusionary principles in criminal cases, but their application in digital surveillance contexts remains underdeveloped. Establishing an independent oversight body—comprising judges, parliamentarians and civil society representatives—with power to audit agencies, investigate abuses and issue binding recommendations would strengthen accountability. Finally, whistle-blower protections should safeguard officials who expose unlawful surveillance. These due process requirements are not merely procedural niceties; they are substantive conditions for the constitutionality of digital surveillance.

VII. Reform Proposals (Normative Recommendations)

To bring Indonesia's surveillance regime into alignment with constitutional and international standards, the following reforms are recommended:

• Adopt a comprehensive Surveillance Warrant Law that consolidates interception, data access and monitoring authorizations. This law should require judicial warrants for any intrusive surveillance, delineate the powers of different agencies and incorporate the four-step proportionality test with procedural safeguards.

• Establish an independent Data Protection Authority with functional and financial autonomy. The authority should issue guidelines, conduct impact assessments, enforce compliance and impose sanctions for violations. Independence from the executive is crucial to avoid conflicts of interest.

• Introduce mandatory transparency mechanisms: annual transparency reports from agencies and service providers detailing surveillance orders and data requests; public parliamentary reporting; and individual notice after surveillance operations conclude.

• Implement strict data retention limits, requiring providers to retain data only for specified periods and anonymize or delete data once it is no longer needed. Mandate end-to-end encryption and prohibit vulnerabilities or backdoor access without court approval.

• Develop oversight bodies composed of judges, legislators and civil society experts. These bodies should have access to classified information, audit surveillance programs, and publish findings. Parliamentary committees can review and approve surveillance budgets and policies.

• Safeguard whistle-blowers and journalists. Legal protections should prevent retaliation against individuals who disclose unlawful surveillance. The Criminal Code's provisions that criminalize defamation and the dissemination of information should be reformed to prevent misuse against critics.

• Enhance algorithmic transparency and fairness by requiring impact assessments for automated profiling systems, prohibiting high-risk inferences, and providing mechanisms for individuals to challenge automated decisions. Promote privacy-by-design and human-rights-by-design in technology procurement.
• Engage civil society and academia in lawmaking. Public consultation and academic research can inform balanced policies that respect rights while addressing security concerns. Comparative insights from countries such as Germany and decisions of the ECHR and the European Court of Justice can guide the design of proportionality and oversight frameworks.
• Harmonize sector-specific laws by removing overlapping mandates and clarifying the roles of the police, intelligence agencies, military and regulators. Ensure that all entities are subject to the same standards of legality, necessity, proportionality and due process.
• Invest in capacity building for judges, lawyers, law enforcement and technologists. Training on digital evidence, privacy implications and human rights law will improve decision-making and implementation.

VIII. Policy Implications

• Enact a unified legal framework that mandates judicial warrants for all intrusive digital surveillance.
• Require service providers to ensure data minimization, purpose limitation, encryption and time-bound retention.
• Guarantee the independence of the forthcoming data protection authority and provide it with enforcement powers.
• Mandate transparency reports and delayed notice to affected individuals to foster accountability and trust.
• Create independent oversight bodies with access to classified information and authority to audit surveillance activities.
• Protect whistle-blowers and journalists to encourage reporting of unlawful surveillance practices.
• Regulate algorithmic profiling through impact assessments, transparency requirements and rights to contest automated decisions.
• Align national laws with international human rights standards, including the ICCPR and the General Data Protection Regulation (GDPR) principles.
• Harmonize sector-specific regulations and clarify institutional mandates to reduce fragmentation and overlap.
• Promote public participation and research in surveillance policymaking and invest in training for judiciary and law enforcement.

IX. Proportionality Checklist for Digital Surveillance

Test Step	Legal Requirement	Procedural Safeguard	Key Questions
Legality	Clear statutory basis	Judicial authorization	Is there an accessible, foreseeable law that authorizes surveillance?
Legitimate aim	National security, public order, rights of others	Explicit statement of purpose	Does the surveillance pursue a concrete, compelling aim?

Necessity	Least intrusive means	Assessment of alternatives	Are less intrusive measures available to achieve the same aim?
Proportionality stricto sensu	Balancing of harms and benefits	Minimization and time limits	Do the benefits outweigh the rights infringements?
Procedural proportionality	Transparency and accountability	Notice, oversight, remedies	Are procedural safeguards in place to protect rights?

X. Conclusion

Indonesia stands at a crossroads in balancing digital surveillance with constitutional rights. The country's legal framework is characterized by fragmented statutes, broad executive discretion and limited judicial oversight. Surveillance practices, including the acquisition of spyware and IMSI catchers and the imposition of regulatory regimes that grant direct access to user data, pose significant threats to privacy, freedom of expression and due process. This paper has argued that the proportionality test—combined with procedural safeguards—provides a robust normative framework for evaluating and limiting state surveillance. Applying this test to targeted, bulk and platform-based monitoring scenarios reveals that many current practices fail to meet constitutional standards of legality, necessity and proportionality. Due process mechanisms, including judicial authorization, specificity, minimization, transparency and remedies, are essential to preserve the rule of law.

The reform proposals and policy implications advanced here offer a roadmap for aligning Indonesian surveillance law with constitutional and international human rights standards. Ultimately, protecting privacy and due process in the digital age requires a cultural shift toward transparency, accountability and rights-respecting governance. Continued research, public engagement and comparative learning will be critical as Indonesia refines its legal architecture and confronts new technological challenges. As the digital landscape evolves, so too must the legal safeguards that protect individuals from unwarranted intrusion and ensure that state power is exercised within constitutional limits.

References

[1] Freedom House. "Indonesia: Freedom on the Net 2023 Country Report." (2023), lines 1061–1074 and 1040–1046 regarding spyware and direct access requirements.
[2] Freedom House. Ibid., lines 1079–1088 regarding the Personal Data Protection Law.
[3] Freedom House. Ibid., lines 1093–1100 concerning data retention and encryption mandates.
[4] Syahwami, S. & Hamirul, H. "The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia," Enigma in Law 2(2) (2024).
[5] UN Human Rights Committee. "General Comment No. 16 on Article 17 (Right to Privacy)." 1988.
[6] Alexy, R. "A Theory of Constitutional Rights." (2002).
[7] Barak, A. "Proportionality: Constitutional Rights and Their Limitations." (2010).
[8] Solove, D. J. "Understanding Privacy." (2008).
[9] Lyon, D. "Surveillance Studies: An Overview." (2007).
[10] United Nations. "Universal Declaration of Human Rights" (1948), Article 12.
[11] International Covenant on Civil and Political Rights (1966), Articles 17 and 19.

[12] European Court of Human Rights. "Klass and Others v. Germany" (1978).
[13] Constitutional Court of the Republic of Indonesia. Selected jurisprudence on privacy and surveillance.
[14] Governmental Regulation No. 71 of 2019 on Electronic Systems and Transactions.
[15] Ministerial Regulation No. 5 of 2020 on Private Electronic System Operators.
[16] Law No. 27 of 2022 on Personal Data Protection.
[17] Electronic Information and Transactions Law (as amended).
[18] Law No. 15 of 2003 on Combating Terrorism.
[19] Law No. 17 of 2011 on State Intelligence.
[20] Comparative jurisprudence: German Federal Constitutional Court decisions on data retention (e.g., 1 BvR 256/08).
[21] European Court of Justice. "Digital Rights Ireland" (Joined Cases C-293/12 and C-594/12).
[22] Article 19. "Legal Analysis: Indonesia—Ministerial Regulation No. 5/2020" (2021).
[23] Freedom House. "Freedom on the Net 2023" overall findings on Indonesia.
[24] Indonesian Criminal Procedure Code and evidence law provisions.
[25] Safenet (Southeast Asia Freedom of Expression Network) reports on digital surveillance and attacks on activists.
[26] Scholarly commentary on proportionality and surveillance in Indonesian context.
[27] Comparative constitutional studies of privacy in Germany, Canada and South Africa.
[28] Report of the UN Special Rapporteur on the Right to Privacy (2019).
[29] European Union. General Data Protection Regulation (GDPR) (2016).
[30] Selected Indonesian Constitutional Court decisions on lawful interception and privacy.