

THE DILEMMA OF AI SURVEILLANCE IN THE RULE OF LAW: CHALLENGES TO PRIVACY RIGHTS AND CIVIL LIBERTIES FROM THE PERSPECTIVES OF INTERNATIONAL AND ASEAN LAW

Samuel Febriyanto

Univeristas 17 Agustus 1945 Jakarta, Indonesia

Email: samuel.febriyantokolopaking@gmail.com

Article History

Received: 18 June 2026

Accepted: 18 July 2026

Published: 01 August 2026

Abstract

The implementation of Artificial Intelligence–based surveillance technologies (AI Surveillance), such as facial recognition and predictive behavioral analysis, has become a primary instrument in maintaining national security. However, the use of these technologies frequently comes into conflict with the protection of human rights. This study is motivated by the growing risk of state transformation into a *surveillance state* capable of conducting mass and automated monitoring of citizens, which may undermine the right to privacy and restrict anonymous freedom of expression in public spaces. The research addresses two main questions: (1) What international standards govern the limitation of AI Surveillance to prevent violations of the right to privacy? and (2) How do ASEAN countries comparatively regulate the accountability of governmental use of surveillance technologies? This research employs a normative juridical method, utilizing a conceptual approach to examine theories of privacy in the digital era, a statutory approach through the analysis of international legal instruments such as the *International Covenant on Civil and Political Rights* (ICCPR), and a comparative approach focusing on ASEAN countries, particularly Indonesia, Singapore, and the Philippines. The findings indicate that most regulatory frameworks in the ASEAN region continue to grant excessively broad discretion to states to conduct surveillance under the justification of national security, often without independent judicial oversight mechanisms. The study concludes that a significant legal gap exists in mitigating discriminatory abuses of AI Surveillance. Accordingly, this research recommends the establishment of a strict “necessity and proportionality test” for all uses of AI in public surveillance, as well as the strengthening of the independence of data protection supervisory authorities at the regional ASEAN level.

Keywords: AI Surveillance, Human Rights, Privacy, International Law.

A. INTRODUCTION

Recent developments in information and communication technology over the past decade have fundamentally transformed the way states perform surveillance and law enforcement functions. Artificial Intelligence (AI) has emerged as a key technology that enables governments to process massive volumes of data (big data) rapidly and automatically. In this context, AI-based surveillance technologies (AI Surveillance) such as facial recognition

technology, movement pattern analysis, and predictive behavioral modelling are regarded as strategic solutions to address national security challenges, transnational crime, and global terrorism.

However, the efficiency and effectiveness of these technologies are not without legal and ethical consequences. The use of AI Surveillance has the potential to fundamentally alter the relationship between the state and its citizens, shifting it from one based on trust to one characterized by permanent suspicion. Governments acquire the capacity to conduct continuous, invisible, and often unnoticed monitoring of individuals. In this context, the right to privacy is no longer understood solely as the protection of personal space but also as the protection of digital identity and the freedom to act anonymously in public spaces.

From a theoretical perspective, this phenomenon represents a shift toward what is commonly referred to as the surveillance state, a condition in which surveillance becomes the primary instrument of state governance. This concept closely resembles the idea of the Panopticon, originally proposed by Jeremy Bentham and later developed by Michel Foucault, in which individuals discipline themselves because they believe they are constantly being observed. Within a democratic rule-of-law framework, such conditions may produce a chilling effect, whereby citizens become reluctant to express their opinions, assemble, or participate in public life due to fear of being monitored and recorded by the state.

From a human rights perspective, the use of AI Surveillance presents a significant dilemma. On the one hand, the state has a positive obligation to protect its citizens from security threats. On the other hand, it is equally bound by the obligation to respect and protect fundamental rights, including the rights to privacy, freedom of expression, and peaceful assembly. The tension between these competing interests becomes increasingly pronounced as AI technologies enable surveillance to be conducted on a mass scale, without specific targeting, and through algorithmic systems that are often opaque and lacking in transparency.

Under international law, the right to privacy has long been recognized as an integral component of universal human rights. International legal instruments affirm that any restriction on the right to privacy is permissible only when it satisfies strict requirements, including a clear legal basis, a legitimate objective, and compliance with the principles of necessity and proportionality. Nevertheless, applying these principles in the context of AI Surveillance presents new challenges, particularly due to the complex, autonomous, and difficult-to-audit nature of AI technologies.

In Southeast Asia, particularly within the Association of Southeast Asian Nations (ASEAN), AI Surveillance has become a highly relevant issue. ASEAN member states are experiencing rapid digital transformation across economic sectors, public services, and national security. Initiatives such as Smart City and Smart Nation have accelerated the integration of surveillance technologies into everyday life. However, the development of legal frameworks governing digital rights protection and state accountability has not kept pace with the rapid adoption of these technologies.

Furthermore, the diverse political and legal systems of ASEAN member states significantly influence how surveillance is implemented and regulated. While some countries have relatively well-established constitutional democratic traditions, others continue to face substantial challenges in upholding human rights and the rule of law. In such contexts, national

security is frequently invoked as a justification for broad surveillance practices carried out without adequate judicial oversight.

Indonesia, Singapore, and the Philippines provide compelling case studies for comparative analysis. Although all three countries have adopted modern surveillance technologies, they differ considerably in their legal frameworks and levels of governmental accountability. Indonesia has enacted the Personal Data Protection Law, Singapore is recognized for its robust and efficient security-oriented approach, while the Philippines possesses a relatively progressive privacy law but continues to encounter significant challenges in its implementation. These differences provide valuable insight into the extent to which the law can function as an instrument for limiting state power in the era of artificial intelligence.

Moreover, a comparative approach illustrates how the concept of the *Rechtsstaat* or Rule of Law is interpreted differently in the context of AI technologies. In Indonesia, for example, the formal recognition of the right to privacy through the Personal Data Protection Law has not yet been accompanied by stringent limitations on the powers of security agencies. In Singapore, efficiency and stability are prioritized, resulting in national security interests often taking precedence over individual rights. Meanwhile, the Philippines presents a paradox between its relatively progressive legal framework and the weak enforcement of its legal protections in practice.

Based on the foregoing discussion, it can be concluded that AI Surveillance is not merely a technical issue or a matter of security policy; rather, it constitutes a structural legal and human rights challenge. Accordingly, comprehensive legal analysis is required to evaluate whether AI Surveillance practices are consistent with the principles of the rule of law, international human rights standards, and the evolving regional dynamics within ASEAN.

B. LITERATURE REVIEW

Privacy Theory

Privacy is a fundamental right inherent to every individual, ensuring protection of personal life, family, communications, and personal data from arbitrary interference. In the digital era, the concept of privacy extends beyond physical space to include the protection of digital identity, personal information, and online activities. Westin (1967) defines privacy as the individual's ability to determine when, how, and to what extent information about themselves is communicated to others. The protection of privacy has become increasingly important with the advancement of Artificial Intelligence (AI), which enables the large-scale collection, analysis, and automated processing of personal data. Therefore, under international law, the right to privacy is recognized as a fundamental human right that may only be restricted based on the principles of legality, necessity, and proportionality (Westin, 1967; United Nations, 1966). Indicators of Privacy Theory

- Protection of personal data.
- Freedom from arbitrary interference.
- Individual control over personal information.
- Consent in data processing.
- Security and confidentiality of personal information.

Rule of Law Theory (*Rechtsstaat*)

The Rule of Law theory asserts that all governmental actions must be based on law and subject to limitations designed to protect the rights of citizens. According to Dicey (1885), the Rule of Law is founded upon three fundamental principles: the supremacy of law, equality before the law, and the protection of individual rights through due legal process. In its contemporary development, the Rule of Law requires not only that governments act in accordance with legal norms but also that they uphold accountability, transparency, and effective oversight of public authority. In the context of AI Surveillance, this theory provides the normative framework for assessing whether surveillance technologies comply with the principles of legality, accountability, and human rights protection. Consequently, governments must not employ AI Surveillance arbitrarily without a clear legal basis and independent oversight mechanisms (Dicey, 1885; Tamanaha, 2004). Indicators of Rule of Law Theory

- Supremacy of law.
- Equality before the law.
- Protection of human rights.
- Government accountability.
- Oversight of governmental authority.

Surveillance Theory (Panopticon and Surveillance Society)

Surveillance Theory explains that monitoring serves as a mechanism for regulating individual behavior through continuous observation. Jeremy Bentham first introduced the concept of the Panopticon, a model of surveillance in which individuals discipline themselves because they believe they are constantly being watched. Michel Foucault (1977) later expanded this concept by arguing that modern surveillance operates not only through physical control but also through social and technological mechanisms that shape human behavior and compliance. Furthermore, Lyon (2001) introduced the concept of the Surveillance Society, describing a society in which people's activities are systematically monitored through digital technologies and data processing systems. In the context of AI Surveillance, this theory explains how artificial intelligence enables governments to conduct large-scale, automated, and continuous surveillance, potentially affecting civil liberties and individuals' right to privacy (Foucault, 1977; Lyon, 2001). Indicators of Surveillance Theory

- Intensity of surveillance.
- Use of surveillance technologies.
- Data collection and analysis.
- Social control through surveillance.
- Impact of surveillance on individual freedom.

C. RESEARCH METHODOLOGY

This study employs a normative-juridical method. The approaches utilized include a conceptual approach examining the theory of the right to privacy and the principle of proportionality a statutory approach involving the analysis of international legal instruments such as the International Covenant on Civil and Political Rights (ICCPR), and a comparative approach regarding surveillance regulations and practices in Indonesia, Singapore, and the Philippines.

D. RESULT AND DISCUSSION

International Standards: The Necessity and Proportionality Test

The right to privacy is one of the fundamental human rights recognized within the international legal system. It is understood not only as the protection of an individual's physical private sphere but also as the protection of personal identity, data, and activities in the digital environment. The rapid advancement of information technology, particularly artificial intelligence (AI), has expanded the scope of privacy rights, thereby requiring a more progressive and contextual interpretation of the law.

International recognition of the right to privacy is explicitly provided under Article 12 of the Universal Declaration of Human Rights (UDHR) and further reinforced by Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR stipulates that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence and that everyone has the right to legal protection against such interference or attacks. This provision imposes a dual obligation upon states: a negative obligation to refrain from arbitrary interference and a positive obligation to establish effective legal mechanisms for the protection of privacy.

In the context of AI Surveillance, the concept of "interference" has undergone a significant transformation compared with conventional forms of surveillance. State interference is no longer confined to physical actions, such as searches or case-specific wiretapping, but now encompasses the systematic, continuous, and often automated collection, processing, and analysis of personal data. Through the application of algorithms and artificial intelligence, governments are capable of constructing individuals' digital profiles, mapping patterns of movement, and predicting behavioral tendencies without any direct interaction between law enforcement authorities and the individuals being monitored.

This expanded interpretation of interference gives rise to significant legal implications due to the covert and imperceptible nature of AI Surveillance. Unlike traditional surveillance, which individuals can generally detect or perceive, AI-based surveillance frequently operates without the knowledge or awareness of the data subject. Such circumstances may effectively deprive individuals of their ability to provide meaningful consent or to challenge the legality of surveillance measures directed against them. From the perspective of international human rights law, such practices may be regarded as arbitrary interference, even when they are carried out under the authority of domestic legislation (David Lyon, 2001).

Furthermore, AI Surveillance extends the scope of state interference beyond the mere collection of information to encompass data-driven decision-making. Algorithmic analyses are increasingly used as the basis for determining security policies, law enforcement strategies, and the classification of individuals or groups according to perceived levels of risk. When such processes are conducted without algorithmic transparency, accountability mechanisms, and adequate judicial oversight, they threaten not only the right to privacy but also the principles of due process of law and equality before the law. Consequently, international law demands a more rigorous interpretation of the concept of interference in the AI era to ensure that technological advancement does not undermine the essence of human rights protection and the principles of the rule of law.

Another equally significant implication is the paradigm shift in law enforcement from an act-based enforcement approach toward predictive enforcement. Within the framework of AI Surveillance, individuals or groups may become targets of state intervention not because they have committed unlawful acts, but because algorithmic analysis predicts that they are likely to do so based on specific data patterns. This predictive approach raises serious concerns regarding the presumption of innocence, a fundamental principle of both the rule of law and international human rights law (UNGA, 2018).

Furthermore, reliance on algorithmic systems in public decision-making carries the risk of creating what is commonly referred to as *black box governance*, a condition in which governmental decision-making processes cannot be effectively understood, scrutinized, or held accountable by the public (Sandra et al., 2017). When individuals are unaware of the algorithmic basis upon which they are placed under surveillance, classified as high-risk, or targeted for law enforcement action, their access to justice is significantly undermined. In such circumstances, the right to an effective remedy, as guaranteed under international human rights instruments, loses much of its substantive meaning.

Accordingly, a strict interpretation of the concept of "interference" under Article 17 of the ICCPR cannot be separated from the state's obligation to ensure adequate procedural safeguards. Protecting the right to privacy in the age of AI requires more than merely establishing normative legal provisions; it must also be supported by mechanisms for transparency, algorithmic auditing, and independent and effective judicial oversight. Without such procedural protections, AI Surveillance risks becoming an instrument of governmental power that operates covertly while exerting far-reaching effects on civil liberties and the quality of democracy.

Beyond procedural concerns, AI Surveillance also raises fundamental questions regarding state accountability in the exercise of public power. In traditional legal systems, the causal relationship between the actions of public authorities and the legal consequences experienced by individuals can generally be traced. However, when state decisions are mediated through complex algorithmic systems, accountability becomes increasingly obscured. Governments may shield themselves behind claims of technological objectivity, while individuals who suffer harm face considerable difficulty in identifying who should be held responsible—the algorithm's developer, the system operator, or the state institution itself. This ambiguity is incompatible with the principle of accountability, which constitutes a cornerstone of both the rule of law and democratic governance.

Furthermore, the large-scale deployment of AI Surveillance has broader implications for the rights to freedom of expression and freedom of peaceful assembly, even where those rights are not directly restricted. The awareness—or even the suspicion—that activities conducted in public spaces are continuously monitored and analyzed by AI systems may encourage individuals to engage in self-censorship. From the perspective of international human rights law, such indirect effects must also be regarded as substantive restrictions on fundamental rights. International human rights courts have consistently recognized that limitations on rights need not always be explicit; they may also arise through state policies or practices that generate fear and uncertainty among the public.

For this reason, international standards increasingly emphasize that the use of AI-based surveillance technologies should be understood as a structural intervention affecting fundamental rights rather than merely as a technical instrument of public security. States are therefore required to conduct a Human Rights Impact Assessment (HRIA) before deploying AI Surveillance, particularly in public spaces. Such assessments should include analyses of potential risks to privacy, non-discrimination, civil liberties, and the effectiveness of oversight and remedial mechanisms. Without a comprehensive, human rights-based approach, the use of AI Surveillance risks reducing the principle of the rule of law to little more than a formal justification for excessive surveillance practices.

Comparative Study in ASEAN: Between Security and Accountability

Through its Smart Nation initiative, Singapore has adopted a highly progressive technological approach to public security and governance. The Singaporean government has integrated thousands of public surveillance cameras with artificial intelligence systems capable of conducting real-time visual analytics, including facial recognition, movement tracking, and the detection of behaviors considered suspicious. These technologies are employed not only for law enforcement purposes but also for traffic management, crowd control, and rapid responses to security incidents. This approach reflects a governance model that prioritizes efficiency, stability, and prevention as the primary objectives of surveillance technology.

From a legal perspective, personal data protection in Singapore is governed by the Personal Data Protection Act (PDPA). However, the PDPA provides broad exemptions permitting the government to process personal data for purposes of national security and public order. In practice, these exemptions place AI Surveillance activities largely beyond the reach of effective public oversight. Citizens have only limited opportunities to challenge or seek judicial review of state surveillance practices, particularly where such surveillance is justified on national security grounds. This situation reflects a significant imbalance of power between the state and individuals in the context of privacy protection.

Moreover, Singapore's surveillance model reflects a paradigm of security-oriented governance, in which the legitimacy of surveillance technologies is measured primarily by their effectiveness in maintaining public order and security rather than by the extent to which they respect fundamental rights. The absence of strong and independent judicial oversight over AI Surveillance raises significant concerns from the perspective of international human rights law (Graham, 2014). Although Singapore's approach has been relatively successful in fostering public safety and social compliance, it risks blurring the line between legitimate surveillance and excessive state interference with citizens' private lives, particularly when AI technologies operate on a massive scale without sufficient transparency.

Following the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), Indonesia has made significant normative progress in recognizing and protecting the right to privacy in the digital era. The PDP Law explicitly classifies biometric data, including facial recognition data, as specific categories of personal data that require enhanced legal protection. This recognition is consistent with evolving international standards, which regard biometric data as high-risk data due to its potential use in AI-based surveillance systems. Conceptually, the enactment of the PDP Law strengthens Indonesia's rule-of-law framework by providing a

legal foundation for addressing the challenges posed by AI Surveillance through data protection mechanisms.

Nevertheless, this normative progress is constrained by the broad exemption contained in Article 50 of the Personal Data Protection Law, which permits the processing of personal data for purposes of national defense and security. The broad and open-ended formulation of this provision raises serious concerns regarding the principles of legality and legal certainty. In the absence of a clear definition of "national security interests" and without a requirement for judicial authorization, this exemption may serve to legitimize preventive and mass AI Surveillance practices. Consequently, technologies such as facial recognition and AI-based behavioral analysis may be deployed without adequate oversight mechanisms, thereby blurring the distinction between legitimate surveillance and excessive state interference with citizens' privacy rights.

Furthermore, these regulatory shortcomings are exacerbated by the lack of an effective independent oversight mechanism for implementing the PDP Law. Although the legislation mandates the establishment of a personal data protection supervisory authority, its effectiveness and institutional independence remain uncertain, particularly in cases involving national security agencies. This situation has created an implementation gap between normative legal protection and actual practice (Bivitri, 2022). From the perspective of international human rights law, the use of AI Surveillance without judicial authorization and independent oversight is inconsistent with the principles of necessity and proportionality. Accordingly, the Indonesian case demonstrates that the existence of data protection legislation alone is insufficient to prevent abuses of AI Surveillance if national security exemptions are not narrowly defined and effectively supervised.

The Philippines is often regarded as one of the ASEAN countries with a relatively progressive legal framework for personal data protection. The Data Privacy Act of 2012 explicitly recognizes the right to privacy as a fundamental right and established the National Privacy Commission (NPC) as an independent supervisory authority responsible for overseeing data processing activities in both the public and private sectors. The Act also incorporates key data protection principles, including transparency, accountability, and purpose limitation. Normatively, this legal framework is consistent with international standards on privacy protection and provides a strong legal basis for limiting the state's use of AI-based surveillance technologies.

However, in practice, the use of surveillance technologies in the Philippines has frequently been associated with serious human rights concerns, particularly in the context of domestic security operations. The war on drugs and counterinsurgency campaigns have involved extensive data collection, digital monitoring, and surveillance technologies implemented with minimal transparency and without effective judicial oversight. Numerous international reports indicate that these surveillance practices have been used to identify, track, and classify individuals or groups as security threats, often resulting in repressive actions (UNHRC, 2020). This situation illustrates a significant gap between normative legal protections and the realities of law enforcement.

Furthermore, the limited accountability of security agencies in deploying surveillance technologies highlights the institutional constraints faced by the National Privacy Commission

when dealing with powerful state actors. Although the NPC possesses administrative authority, its capacity to effectively oversee large-scale security operations remains limited. From the perspective of international human rights law, this situation demonstrates the state's failure to fulfill its positive obligation to effectively protect both the right to privacy and the right to life. Accordingly, the Philippine experience illustrates that the existence of progressive privacy legislation does not, in itself, guarantee effective human rights protection unless it is supported by independent law enforcement, robust accountability mechanisms, and meaningful judicial oversight of the state's use of AI Surveillance.

E. CONCLUSION

The development and implementation of Artificial Intelligence (AI)-based surveillance technologies (AI Surveillance) have introduced existential challenges to the traditional concept of human rights, particularly the rights to privacy and civil liberties. Under the classical legal framework, restrictions on the right to privacy have generally been understood as case-specific and limited forms of state intervention. However, AI Surveillance introduces a model of surveillance that is systemic, large-scale, and continuous, thereby transforming state interference from isolated actions into a mechanism of structural control. This transformation necessitates a reinterpretation of established human rights principles to ensure their continued relevance in the face of technologies capable of automatically and predictively collecting, processing, and analyzing individuals' data.

International legal standards, particularly those derived from the International Covenant on Civil and Political Rights (ICCPR), provide a relatively clear normative framework for limiting the state's use of surveillance technologies. The principles of legality, necessity, and proportionality constitute the fundamental conditions under which restrictions on the right to privacy may be considered legally justifiable. Furthermore, international law emphasizes the importance of independent oversight mechanisms and judicial control as essential safeguards against the potential abuse of state power. Nevertheless, this study demonstrates that the incorporation of these international standards into the domestic legal systems of ASEAN member states continues to face significant challenges at both the normative and implementation levels.

Within the ASEAN region, there is a strong tendency to prioritize national security and social stability over the protection of individual privacy rights. This tendency is reflected in the fragmented nature of personal data protection regulations, the broad exemptions granted to state authorities, and the weak accountability mechanisms governing the use of surveillance technologies. The comparative analysis of Indonesia, Singapore, and the Philippines reveals a common pattern despite important contextual differences. Indonesia faces the challenge of excessively broad national security exemptions under its Personal Data Protection Law; Singapore employs surveillance as an efficient governance tool while maintaining limited judicial oversight; and the Philippines exhibits a pronounced gap between its progressive legal framework and the weak enforcement of laws against state actors.

These findings indicate that AI Surveillance within the ASEAN region continues to operate within a legal framework that remains insufficiently developed. When surveillance

technologies are deployed without transparency, judicial authorization, and effective independent oversight, the risk of human rights violations increases substantially. Preventive and mass surveillance practices are capable of generating a chilling effect, undermining freedom of expression, freedom of peaceful assembly, and public participation in democratic life. In the long term, such practices threaten not only individual rights but also weaken the very foundations of the rule of law and democratic governance.

Accordingly, it can be concluded that the principal challenge posed by AI Surveillance lies not merely in the sophistication of the technology itself, but rather in the inadequacy of existing legal and institutional frameworks to regulate and constrain its use. Without a strong commitment to maintaining the law as an instrument for limiting state power, AI Surveillance risks becoming a mechanism of social control that is incompatible with the universal values of human rights. Therefore, strengthening legal standards, oversight mechanisms, and state accountability constitutes an essential prerequisite for ensuring that the development and deployment of AI technologies do not come at the expense of the fundamental principles of human rights protection and democracy.

Based on the findings and analysis of this study, concrete and systematic measures are required to ensure that the use of AI Surveillance technologies does not evolve without effective oversight or erode the fundamental principles of the rule of law and the protection of human rights. The recommendations proposed are directed not only at the national level of individual ASEAN member states but also at the regional level, reflecting the inherently transboundary nature of digital technologies.

First, ASEAN governments are encouraged to adopt a temporary moratorium on the deployment of Facial Recognition Technology (FRT) in public spaces. Such a moratorium represents a precautionary approach, given the significant risks associated with violations of privacy rights, algorithmic bias, and the misuse of biometric data. The moratorium should not be understood as a permanent rejection of the technology but rather as a regulatory pause until a comprehensive legal framework has been established. This framework should include mandatory independent algorithmic audits, transparency requirements for AI systems, and strict limitations on the purposes of surveillance as well as data retention periods. Without these safeguards, the use of FRT in public spaces risks becoming a form of mass surveillance that is inconsistent with the principles of necessity and proportionality under international human rights law.

Second, the establishment and strengthening of independent data protection supervisory authorities, free from executive influence, should become a priority across ASEAN member states. These supervisory bodies must be vested with clear legal authority to oversee how data generated through AI Surveillance are collected, processed, stored, and utilized by law enforcement agencies and national security institutions. Institutional independence is essential to enable these authorities to effectively perform their oversight functions, including conducting investigations, imposing sanctions, and receiving complaints from the public. Without genuinely independent oversight, data protection legislation risks becoming merely symbolic, incapable of preventing national security interests from overriding individuals' rights to privacy.

Third, at the regional level, ASEAN should be encouraged to develop a common normative instrument in the form of an ASEAN Declaration on Digital Rights. Such a declaration should establish minimum ethical and legal standards governing the use of AI technologies, particularly for state-led mass surveillance. The adoption of regional standards is crucial in light of the regulatory disparities among ASEAN member states and the cross-border nature of digital technologies and data flows. The declaration could serve as a common framework for balancing national security interests with the protection of human rights while reinforcing ASEAN's commitment to the principles of democracy and the rule of law in the digital era.

Overall, these recommendations underscore that the governance of AI Surveillance requires a multi-level approach that combines national legal reforms with regional normative initiatives. Without such measures, the normalization of mass surveillance will become increasingly likely, leaving human rights protection within the ASEAN region in a persistently vulnerable position. Accordingly, these recommendations are intended to provide practical guidance for policymakers, academics, and civil society in developing human-centered AI governance that is consistent with the principles of the rule of law and the protection of fundamental human rights.

REFERENCES

- Bentham, Jeremy. *Panopticon; or, The Inspection-House*. London: T. Payne, 1791.
- Bivitri Susanti, "The Implementation Gap of Data Protection Law in Indonesia," *Indonesia Law Review* 12, no. 3 (2022): 345–360.
- Chesterman, Simon. *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty*. Oxford: Oxford University Press, 2011.
- Dicey, A. V. (1885). *Introduction to the study of the law of the constitution*. Macmillan.
- Djafar, Wahyudi. "Hak atas Privasi dan Perlindungan Data Pribadi di Indonesia." *Jurnal HAM* 10, no. 2 (2019): 123–138.
- David Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001), 56–59.
- Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books, 1995.
- Government of Singapore, *Smart Nation: The Way Forward* (Singapore: Prime Minister's Office, 2018).
- Greenleaf, Graham. *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford: Oxford University Press, 2014.
- Human Rights Watch. "License to Kill": *Philippine Police Killings in Duterte's "War on Drugs"*. New York: Human Rights Watch, 2017.
- Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
- Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 50.
- Kaye, David. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. UN Doc. A/HRC/41/35. Geneva: United Nations, 2019.

- National Privacy Commission (Philippines). *Implementing Rules and Regulations of the Data Privacy Act of 2012*. Manila, 2016.
- Republic of the Philippines. *Data Privacy Act of 2012* (Republic Act No. 10173).
- Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,” *International Data Privacy Law* 7, no. 2 (2017): 76–99
- Simon Chesterman, *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (Oxford: Oxford University Press, 2011), 84–92.
- Singapore. *Personal Data Protection Act 2012*. Singapore Statutes.
- Tamanaha, B. Z. (2004). *On the rule of law: History, politics, theory*. Cambridge University Press.
- United Nations, *International Covenant on Civil and Political Rights*, 16 December 1966, 999 UNTS 171, art. 17.
- United Nations. *International Covenant on Civil and Political Rights*. New York: United Nations, 1966.
- United Nations, *Universal Declaration of Human Rights*, GA Res. 217 A (III), 10 December 1948, art. 12.
- United Nations. *Universal Declaration of Human Rights*. New York: United Nations, 1948.
- United Nations Human Rights Committee. *General Comment No. 16: Article 17 (Right to Privacy)*. UN Doc. HRI/GEN/1/Rev.9 (Vol. I). Geneva: United Nations, 1988.
- United Nations General Assembly, *The Right to Privacy in the Digital Age*, UN Doc. A/RES/73/179, 17 December 2018.
- United Nations Human Rights Council. *Report of the Special Rapporteur on the Right to Privacy*. UN Doc. A/HRC/48/31. Geneva: United Nations, 2021.
- United Nations Human Rights Council. *Report of the United Nations High Commissioner for Human Rights on the Situation of Human Rights in the Philippines*. UN Doc. A/HRC/44/22. Geneva: United Nations, 2020.
- United Nations Human Rights Council, *Report of the United Nations High Commissioner for Human Rights on the Situation of Human Rights in the Philippines*, UN Doc. A/HRC/44/22 (2020), paras. 56–61
- United Nations. (1966). *International Covenant on Civil and Political Rights*. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>