The System Paradigm in AI Ethics and Infrastructure Governance: An Analysis of the Role of the Operating System

Fiqla Syabifi[1], Muhammad Febriansyah[2], Fadlan Nur Alifiansyah[3], Elevina Zukhruf[4]
[1,2,3,4]Information Systems and Technology/Faculty of Engineering, Universitas Negeri Jakarta
fiqlacampus24@gmail.com[1], 2014519.muhammadfebriansyah@gmail.com[2],
fadlanalifiansyah@gmail.com[3], elev1na.zukhruf@gmail.com[4]

Submitted: June 26, 2026; accepted: May 5, 2026

Abstract

The rapid development of artificial intelligence (AI) has had a transformational impact across various sectors, yet it simultaneously raises multidimensional challenges, particularly in terms of ethics and infrastructure governance. This study aims to analyze AI governance through a system paradigm approach, using the operating system (OS) as an analytical analogy. A qualitative method was employed through a literature review of reputable journals and academic databases addressing AI ethics, the system paradigm, and infrastructure governance. The results show that the system paradigm provides a holistic framework for integrating ethical principles, regulatory mechanisms, and technical functions within the AI ecosystem. The OS analogy highlights the importance of governance components such as an ethical kernel, access control, and security layers to ensure transparency, accountability, and fairness. This study concludes that responsible AI governance requires a systemic, adaptive, and sustainability-oriented approach that bridges technological innovation with social and ethical values.

Keywords: Artificial Intelligence, System Paradigm, AI Governance, Operating System, Ethics

1. Introduction

The development of artificial intelligence (*Artificial Intelligence*/AI) over the past decade has had a transformational impact on many aspects of human life. From industrial automation and data-driven healthcare to public decision-making, AI serves as a catalyst for digital transformation that accelerates efficiency and innovation. However, this acceleration also brings multidimensional challenges, particularly concerning ethical issues such as algorithmic bias, privacy, and accountability, as well as technical infrastructure issues including stability, security, and computing capacity [1].

Within the framework of the philosophy of science, the emergence of AI can be understood as a scientific paradigm shift as described by Thomas Kuhn in The Structure of Scientific Revolutions. Kuhn rejected the linear, cumulative view of scientific progress and emphasized that scientific transformation occurs through paradigm revolutions when anomalies can no longer be explained by the old framework. In the context of AI, this paradigm shifts the focus from systems based on explicit rules toward adaptive and autonomous learning systems, which change not only technology but also social and policy perspectives on technology [2].

Although academic research on AI has grown rapidly, attention to the ethical and governance dimensions at the level of technical infrastructure remains relatively limited. Yet the operating system (OS), as core software, plays a strategic role in managing computing resources, hardware communication, and data access control. Without an operating system that integrates the principles of ethics, transparency, and security, the deployment of AI may pose serious risks, both technical and social [3].

Furthermore, the urgency of ethical AI governance becomes increasingly evident when this technology is applied to public policy decision-making. Several studies emphasize that the use of AI without a clear ethical framework can reinforce structural bias, reduce accountability, and raise legitimacy problems in government decisions. Therefore, the integration of both international and national ethical frameworks, such as the UNESCO recommendation and Indonesia's national AI ethics guidelines, is needed to ensure that AI is applied responsibly and benefits society [3].

Accordingly, an approach based on the system paradigm is needed to understand the complexity of AI governance. This paradigm views AI not merely as a product of algorithms and hardware, but as part of a socio-technological ecosystem that involves regulations, policies, normative values, and supporting infrastructure. From this perspective, the operating system can be seen as a foundation that

not only supports technical stability but also serves as a conceptual instrument for organizing AI ethics and governance more comprehensively.

2. Research Method

This study used a qualitative approach with a literature review method. This approach was chosen because it is suitable for exploring theoretical concepts and analytical frameworks related to the ethical governance and infrastructure of artificial intelligence (*Artificial Intelligence*/AI). The research data were obtained from secondary sources in the form of scientific journal articles, conference proceedings, and reports from international institutions published over the last 10 years (2015–2025). The literature selection criteria were: (1) published in a reputable journal and assigned a Digital Object Identifier (DOI); (2) addressing *AI Ethics*, *System Paradigm*, *AI Governance*, or *AI Infrastructure*; and (3) relevant to an analytical framework based on the operating system analogy.

The analysis procedure was carried out in three stages. First, literature was collected using keywords such as *AI Ethics, System Paradigm, AI Governance,* and *AI Infrastructure* in international academic databases (Scopus, IEEE Xplore, SpringerLink, ScienceDirect) and a national portal (SINTA) for Indonesian-language literature. Second, a critical evaluation of the literature was conducted to identify the main ideas, research gaps, and theoretical contributions of each article. Third, a thematic synthesis was performed by organizing the findings into the categories of ethics, infrastructure, and the system paradigm, and then linking them to the operating system analogy. The entire analysis was conducted in a descriptive-qualitative manner, with the aim of producing a comprehensive conceptual framework for AI governance.

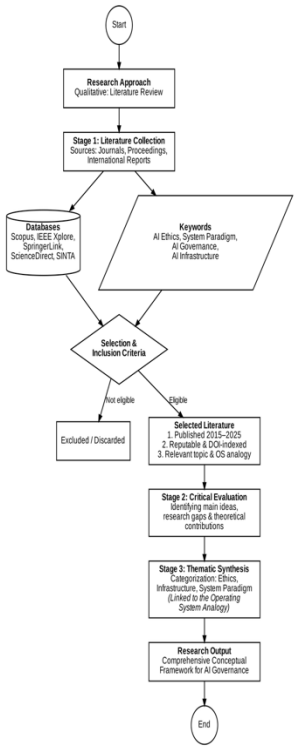


Figure 1. Research Flow

1. **Stage I: Initiation & Design**
   a) Start: Defining the research design using a qualitative approach with a literature review method.
   b) Focus: Exploring theoretical concepts of the ethical governance and infrastructure of AI.
2. **Stage II: Data Collection**
   a) Data Sources: Secondary data (journal articles, proceedings, institutional reports).

b) Databases: Searching Scopus, IEEE Xplore, SpringerLink, ScienceDirect (international) and SINTA (national).
c) Keywords: Using the search queries "*AI Ethics*", "*System Paradigm*", "*AI Governance*", and "*AI Infrastructure*".

3. **Stage III: Selection (Filtering)**
   a) The literature was filtered based on the following inclusion criteria:
   b) Published within the last 10 years (2015–2025).
   c) Good reputation and a Digital Object Identifier (DOI).
   d) Substance relevant to the topic and to the operating system analogy framework.
4. **Stage IV: Data Analysis (Procedure)**
   a) Critical Evaluation: Examining the literature to identify the main ideas and research *gaps*.
   b) Thematic Synthesis: Grouping the findings into the categories of Ethics, Infrastructure, and System Paradigm, then linking them through the Operating System Analogy.
5. **Stage V: Results**
   Output: A comprehensive conceptual framework for AI governance.

3. Results and Discussion

3.1 The System Paradigm: Definition and Relevance to AI

The system paradigm is rooted in general systems theory, which emphasizes interconnectedness, interdependence, and *feedback loops* among elements. A system cannot be understood merely by examining its components separately; rather, it must be viewed through the dynamic interactions among the parts that form the whole. Since 1962, Herbert Simon has emphasized that "*the whole is more than the sum of its parts*" within the framework of complexity, an idea that has since been widely adopted in studies of modern technology. In the context of artificial intelligence (AI), the system paradigm positions ethics, technological infrastructure, policy, and social actors as interrelated subsystems, so that a failure in one subsystem can create a domino effect on the entire system [4].

The systemic approach also requires that technological phenomena be viewed not only from a technical standpoint but as part of an interacting social, cultural, and historical environment. This paradigm emphasizes that information systems, including AI, are not merely software or technical infrastructure but also encompass social and institutional cooperation. This perspective shifts the way information systems are researched: from mere technicalities toward an analysis of social relations, ideological goals, and ethical and cultural impacts [5].

Over time, the system paradigm can be read through the lens of Thomas Kuhn's epistemology. AI emerged as a "new paradigm" after traditional deterministic computing faced a crisis caused by the complexity of *big data*. The emergence of *machine learning* and *neural networks* represents a revolution that has produced a shift in thinking while marking a new normal in modern science. Today, AI not only accelerates research and data analysis but also shapes patterns of global social, political, and economic interaction. On the other hand, challenges such as algorithmic bias, transparency, and accountability underscore the need for ethical governance grounded in the system paradigm [6].

The relevance of the system paradigm becomes even clearer when AI is understood as a *sociotechnical system*. This means that technology does not stand alone but is always embedded in a network of institutions, cultures, regulations, and social practices. For example, a fraud detection algorithm depends not only on technical metrics but also on the political context, the behavior of bureaucrats, and the applicable legal regulations. Thus, adopting the system paradigm helps highlight that the success or failure of AI depends on the configuration of complex interactions between technical and non-technical components [6].

3.2 AI Ethics Governance from a Systems Perspective

AI ethics is often understood as a set of normative principles such as transparency, fairness, accountability, and non-discrimination. However, within the system paradigm, ethics is not merely a set of abstract rules; rather, it functions as a controlling *layer* that interacts with various actors: regulators who set policies, technology developers who design algorithms, and society as the recipient

of direct impacts. Thus, AI ethics governance should be viewed as a relational network that requires cross-actor collaboration to achieve a balance between innovation and the protection of social values [7].

A systemic approach helps map the interrelationships among these actors. For instance, a regulator's failure to formulate data privacy rules can create the risk of ethical violations, which in turn reduces public trust in developers and AI systems. Research on Responsible AI Governance shows that effective governance mechanisms must answer fundamental questions: who is responsible, what is controlled (people, data, processes, systems), when oversight takes place throughout the AI lifecycle, and how control mechanisms are implemented through policies, standards, and regulations [8]. This model affirms that ethics governance is not only a matter of legal regulation but also the integration of practices across the stages of system development.

In terms of implementation, major challenges arise in the domain of social media and digital platforms. AI algorithms are used to personalize content, increase engagement, and drive virality. Although beneficial, these systems raise ethical problems in the form of algorithmic bias, lack of transparency, and privacy violations. Recent studies confirm that algorithms can narrow the diversity of information by displaying only content based on prior preferences, while also opening opportunities for the misuse of user data [9]. A systems perspective highlights that this problem cannot be placed solely on platforms; it requires the involvement of regulators (through privacy standards), developers (by building transparent algorithms), and society (by improving digital literacy).

In the Indonesian context, the issue of AI ethics is becoming increasingly relevant. Legal research emphasizes that AI raises specific problems that cannot be regulated by public or private governance alone. Therefore, Lex AI is needed, namely a sui generis form of governance with its own legal characteristics that complements the existing regulatory framework [7]. In addition, AI ethics must also be seen as a comprehensive accountability mechanism: ensuring fairness, accountability, transparency, and personal data protection in all phases of development and use [10].

Table 1. Top 10 countries by number of compromised ChatGPT credentials [11]

No	Top countries by number of compromised ChatGPT credentials	
	Country	Number of Stolen Records
1	India	12,632
2	Pakistan	9,217
3	Brazil	6,531
4	Vietnam	4,771
5	Egypt	4,588
6	United States	2,995
7	France	2,923
8	Morocco	2,647
9	Indonesia	2,555
10	Bangladesh	2,463

Data breach cases, such as the compromise of thousands of ChatGPT accounts in various countries including Indonesia, show that ethical threats are not merely hypothetical but real. A security report ranks Indonesia ninth in the world, with 2,555 compromised ChatGPT accounts [11]. This incident shows that weak control at a single point in the system (data security) can affect other subsystems, leading, for example, to a loss of public trust or reduced stability of the digital ecosystem.

3.3 AI Infrastructure and the Operating System Analogy

Artificial intelligence (AI) infrastructure is the technical foundation that enables large-scale data processing and the execution of complex algorithms. The main elements of this infrastructure include *hardware* (CPUs, GPUs, TPUs), data centers, *cloud computing*, networks, and supporting *software*. All of these components need to be managed in an integrated manner to deliver efficient, secure, and scalable AI performance.

From the perspective of the operating system (OS), the role of AI infrastructure can be likened to the function of an OS as a bridge between hardware and applications. The operating system ensures that resources (CPU, memory, *storage*, network) are properly allocated while maintaining system stability and security. By the same analogy, AI ethics governance functions as a "social operating system" that ensures AI applications run according to the rules, upholding *fairness*, transparency, and user data security [12].

Just as an OS has *resource management*, *security*, and *scheduling* modules, AI ethics governance also plays a role in regulating data access, controlling bias, and prioritizing social interests. An OS ensures that no single application dominates system resources; likewise, AI governance must ensure that business interests do not come at the expense of privacy or social justice [13].

Furthermore, a robust AI infrastructure must be integrated with *IT governance*. Research shows that AI can improve IT governance through automation, proactive risk management, and better decision quality. However, challenges such as data privacy and changes in organizational culture still need to be addressed [14]. Thus, the success of AI is determined not only by the sophistication of its algorithms but also by the infrastructure and governance ecosystem that supports it.

In the context of digital transformation, AI deployment, likened to an "application," can only run effectively if it is supported by a stable OS. Recent research confirms that application-based AI can shift the information technology paradigm from reactive to proactive systems oriented toward intelligence and innovation. Nevertheless, infrastructure and governance readiness remain absolute prerequisites for the benefits of AI to be optimized sustainably [14].

3.4 Analysis: The Role of the Operating System in AI Governance

In understanding the governance of AI ethics and infrastructure, the operating system (OS) can serve as a powerful analogy. Just as an OS regulates the interaction between hardware, applications, and users, AI governance also requires mechanisms that integrate ethics, law, and technology.

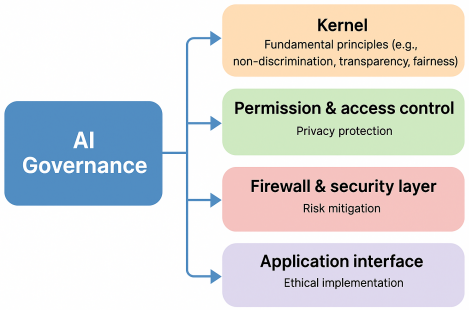


Figure 2. The Operating System Analogy for *AI Governance*

Kernel (core rules). The kernel of an operating system is the control center that determines how the entire system works. In the context of AI governance, the kernel can be likened to fundamental ethical principles such as non-discrimination, transparency, and fairness, which must form the foundation of every AI implementation. Camilleri (2024) emphasizes that AI governance requires universal principles to prevent bias and protect human rights, so that ethics is not merely an add-on but the core of AI infrastructure [15].

Permission & access control. An OS manages user access rights through permissions (*permission*) and access control. This analogy is consistent with the need for AI governance to ensure the protection of data privacy. In Indonesia, although the 2022 Personal Data Protection (PDP) Law is in place, the regulation does not yet fully cover AI-specific issues such as algorithmic accountability and automated decision-making [12]. This indicates that the access control system in AI governance must be more strongly integrated with data protection law in order to meet international standards.

Firewall & *security layer*. In an OS, firewalls and security layers prevent intrusion and misuse. A similar function must also exist in AI governance in the form of risk mitigation mechanisms against misuse, for example in information manipulation or deepfakes. A recent study on AIOS (LLM Agent Operating System) emphasizes the importance of a kernel layer capable of managing *resources*, access, and control to prevent monopolization and potential security vulnerabilities [16]. In other words, the AI governance firewall must be proactive rather than merely reacting after a violation has occurred.

Application interface. The application interface in an OS allows users to interact with the system safely and in a controlled manner. In AI governance, this can be understood as the way ethical principles and regulations are embodied in real products, such as virtual assistants, recommender systems, or AI-based public services. Implementing ethical interfaces ensures that ethical norms do not stop at the policy level but can truly be accessed and experienced by users.

Table 2. The Operating System Analogy for AI Governance

.

No	The Operating System Analogy for AI Governance	
	Operating System	**AI Governance**
1	Kernel	Ethical Principles (transparency, fairness, non-discrimination)
2	Access Control	Regulation & Data Privacy Protection
3	Security Layer	Risk Mitigation (bias, manipulation, deepfakes)
4	Application Interface	Real-World Implementation (AI applications, public services)

With this framework, AI ethics governance can be viewed not merely as a set of norms or laws, but as an operational mechanism embedded in infrastructure, much like an operating system that supports the entire ecosystem of software and hardware.

4. Conclusion

This study shows that an approach based on the system paradigm provides an effective conceptual framework for understanding the complexity of the governance of artificial intelligence ethics and infrastructure. Using the operating system analogy, AI governance can be viewed as a coordination mechanism that integrates ethical principles, regulations, and technical functions so that the AI ecosystem operates in a harmonious, secure, and accountable manner. This analysis confirms that the successful implementation of AI is determined not only by algorithmic advances but also by the quality of governance capable of balancing the need for innovation with the protection of social values. These findings contribute to the development of a more comprehensive, adaptive, and sustainability-oriented AI governance model, while also opening avenues for further research on the application of the system paradigm in public policy and ethical digital infrastructure design.

References

[1] J. Rofifatuz Zahabiyyah and A. Nabila Septiana, "Etika Kecerdasan Buatan Artificial Intelligence (Ai) Dalam Pengambilan Keputusan Kebijakan Publik," 2024.

[2] T. F. Amelia, R. Susanti, Y. Yosef, and S. M. Siahaan, "Perspektif Thomas Kuhn : Epistemologi Paradigma dan Revolusi Kecerdasan Buatan," *JURNAL YAQZHAN: Analisis Filsafat, Agama dan Kemanusiaan*, vol. 10, no. 2, p. 260, Dec. 2024, doi: 10.24235/jy.v10i2.18777.

[3] A. Eda Pradana, A. R. Herawati, I. H. Dwimawanti, and Maesaroh, "Tantangan Kecerdasan Buatan Dalam Implikasi Kebijakan Pemerintah di Indonesia: Studi Literatur," *Jurnal Good Governance*, pp. 51–66, Apr. 2025, doi: 10.32834/gg.v21i1.889.

[4] N. Kolt, M. Shur-Ofry, and R. Cohen, "Lessons from complexity theory for AI governance," Mar. 2025, [Online]. Available: http://arxiv.org/abs/2502.00012

[5] Lolanda Hamim Annisa and Y. H. C. Pratama, "Implementasi Paradigma Interaksi Manusia & Komputer Pada di Era Society 5.0: Systematic Literature Review," *Technology and Informatics Insight Journal*, vol. 1, no. 2, pp. 66–74, Nov. 2022, doi: 10.32639/tiij.v1i2.183.

[6] O. Kudina and I. van de Poel, "A sociotechnical system perspective on AI," *Minds Mach (Dordr)*, vol. 34, no. 3, Sep. 2024, doi: 10.1007/s11023-024-09680-2.

[7] F. Lisaldy, Ismail, and D. Iryani, "Lex AI sebagai Tata Kelola Kecerdasan Buatan Sui Generis di Indonesia," *Technology and Economics Law Journal*, vol. 3, no. 1, 2024, doi: 10.21143/TELJ.vol3.no1.1051.

[8] A. Batool, D. Zowghi, and M. Bano, "Responsible AI Governance: A Systematic Literature Review," 2025, doi: 10.48550/arXiv.2401.10896.

[9] P. Hikmah Febryan, A. Kusuma Negara, and M. Farell Altivan Ramadhan, "ANALISIS PENGGUNAAN AI DALAM ALGORITMA SOSIAL MEDIA : SYSTEMATIC LITERATURE REVIEW," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 1, pp. 1095–1102, Dec. 2024, doi: 10.36040/jati.v9i1.12613.

.

[10] Nasman. Nasman, P. Astuti, and D. Perwitasari, "ETIKA DAN PERTANGGUNGJAWABAN PENGGUNAAN ARTIFICIAL INTELENGENCE DI INDONESIA.," *Jurnal Hukum Lex Generalis*, vol. 5(10), 2024, doi: https://doi.org/10.56370/jhlg.v5i10.

[11] Group-IB, "Group-IB Discovers 100K+ Compromised ChatGPT Accounts on Dark Web Marketplaces; Asia-Pacific region tops the list," Group-IB. [Online]. Available: https://www.group-ib.com/media-center/press-releases/stealers-chatgpt-credentials/

[12] L. Judijanto and R. Madah Khulaili Harsya, "Etika dan Hukum dalam Penggunaan Artificial Intelligence terhadap Privasi Digital di Indonesia," vol. 3, no. 3, pp. 141–149, 2025, doi: 10.58812/shh.v3.i03.

[13] M. F. Adiman, Baharuddin, A. Ikhlas, Muhamad. Sigid Safarudin, S. Muhammad, and D. Kelly Sawlani, "Pengembangan Aplikasi Berbasis Artificial Intelligence (AI) Mengubah Pradigma Tekhnologi Informasi," Dec. 2024. doi: https://doi.org/10.31004/irje.v4i4.1553.

[14] Zulkarnain Zulkarnain, Jesselyn Jesselyn, Hansvirgo Hansvirgo, Fendy Gunawan, and Sandy Alferro Dion, "Peran Artificial Intelligence (AI) dalam Peningkatan IT Governance: Kajian Literatur," *Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika*, vol. 2, no. 3, pp. 62–71, May 2024, doi: 10.61132/merkurius.v2i3.109.

[15] M. A. Camilleri, "Artificial intelligence governance: Ethical considerations and implications for social responsibility," *Expert Syst*, vol. 41, no. 7, Jul. 2024, doi: 10.1111/exsy.13406.

[16] K. Mei *et al.*, "AIOS: LLM Agent Operating System," Mar. 2024, [Online]. Available: http://arxiv.org/abs/2403.16971