World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Governing the Ungovernable: Structural Contradictions, Institutional Limitations, and the Constraints of State Authority in AI Regulation in China and the United States

Jimmy Kinyonyi Bagonza *

Department of Information Technology, School of Computer and Information Science, University of the Cumberlands, Williamsburg, KY, USA.

World Journal of Advanced Research and Reviews, 2026, 30(03), 924-931

Publication history: Received on 30 April 2026; revised on 10 June 2026; accepted on 12 June 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.30.3.1617

Abstract

Both China and the United States have developed complex artificial intelligence (AI) governance frameworks; however, neither system is able to fulfill its stated objectives. This review article employs a comparative political-economy approach to explore how each nation's foundational political structure leads to unique, intractable regulatory failures. In China, the Party-state model creates an innovation-control paradox: the imperatives of information sovereignty embedded in its generative AI regulations and cross-border data transfer restrictions ultimately undermine the open research environments essential for advancing frontier AI development. This situation disproportionately impacts smaller technology companies and academic researchers while reinforcing the dominance of established industry leaders. Conversely, the United States grapples with severe regulatory fragmentation, leaving existing governance gaps that enable persistent cross-sectoral AI risks, as industry lobbying effectively reframes necessary safety regulations as economically unpatriotic. By examining specific legislative instruments, including the Cyberspace Administration of China's 2023 Interim Measures for Generative AI, Executive Order 14110, and using the EU AI Act as a comparative benchmark, this paper evaluates critical friction points in compliance cost distribution, institutional coordination failures, and the macroeconomic repercussions these frameworks impose on emerging markets in Southeast Asia, Sub-Saharan Africa, and Latin America. The paper concludes that meaningful governance progress requires separating information control from technical AI oversight in China, establishing a unified federal AI statute in the United States, and creating multilateral regulatory coalitions. These coalitions would enable emerging economies to maintain policy autonomy while striving for interoperability with leading AI ecosystems.

Keywords: Governance Of Artificial Intelligence; Regulation Comparison; AI Policy In China; AI Policy In The United States; Fragmentation in Regulation; Digital Governance In Emerging Markets

1. Introduction

Artificial intelligence has emerged as the defining technological challenge of the twenty-first century, where economic competitiveness, military superiority, and normative influence intersect in ways that render traditional regulatory frameworks inadequate [1]. Both China and the United States have committed substantial political resources to AI governance, formulating comprehensive policy architectures aimed at reconciling innovation with security, efficiency with accountability, and national interests with global responsibilities. However, beneath these ambitious declarations lies a more concerning reality; both nations have established regulatory systems whose inherent contradictions and institutional limitations systematically undermine their stated objectives.

Analyzing these two nations proves fruitful, as they represent not only contrasting regulatory approaches but also fundamentally different theories of State governance[2]. China's strategy embodies a Leninist developmental model, in

* Corresponding author: Jimmy Kinyonyi Bagonza

which the Party not only sets industrial targets but also asserts its authority to regulate private enterprises pursuing these objectives. In contrast, the United States adheres to a fragmented, sector-specific regulatory framework shaped by constitutional federalism, judicial review, and a deep ideological resistance to anticipatory regulation [3]. These structural differences lead to distinct failure modes rather than establishing a simple hierarchy of effectiveness.

This paper presents three interrelated arguments. First, although both nations frame AI governance as a means to enhance national security and achieve economic superiority, their regulatory frameworks are fundamentally incapable of realizing these objectives due to inherent contradictions within each country's political economy. Second, these contradictions lead to asymmetric compliance costs, disproportionately burdening smaller technology firms, academic researchers, and citizens without significant political influence, rather than imposing these costs on the large incumbent entities that shape the regulatory landscape. Third, the global spillover effects from these contentious governance models create a structural dilemma for emerging markets, necessitating a multilateral institutional response rather than a simple binary alignment with one of the prevailing frameworks.

The paper is organized as follows. Section 2 outlines the policy frameworks and strategic contexts of each nation. Section 3 offers a comprehensive analysis of institutional friction points and discrepancies in compliance costs. Section 4 delivers a comparative political-economic assessment. Section 5 proposes policy revisions, focusing on the associated economic and legal trade-offs. Finally, Section 6 concludes with a discussion on the implications for global technology governance.

2. Policy Frameworks and Strategic Context

2.1. China's AI Governance Framework

China's regulatory approach to artificial intelligence should not be viewed solely as a tool for censorship, but rather as what Ang [4] calls "directed improvisation", a governance model that allows entrepreneurial flexibility within the boundaries set by Party priorities. The 2017 New Generation Artificial Intelligence Development Plan (AIDP) laid out a three-stage roadmap to achieve global leadership in AI by 2030, explicitly linking AI advancement to military-civil fusion and the broader objective of "national rejuvenation"[5]. This plan has been implemented through a series of application-specific regulations, including the 2021 Algorithmic Recommendation Management Provisions, the 2022 Deep Synthesis (deepfake) regulations, and the 2023 Interim Measures for the Management of Generative AI Services issued by the Cyberspace Administration of China (CAC)[6].

The institutional landscape is marked by competing jurisdictions. While the CAC has established itself as the primary regulatory authority for internet-facing AI applications, overlapping mandates persist among the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security, the National Development and Reform Commission (NDRC), and the People's Liberation Army's Strategic Support Force [7]. This fragmentation is somewhat alleviated at the top level by the Party's Central Cybersecurity and Informatization Commission, which plays a role in political coordination. However, as discussed in Section 3, this regulatory framework creates significant compliance challenges for firms operating in a multi-regulator environment.

China's strategic motivations are rooted in a dual imperative. Economically, AI is viewed as crucial for sustaining growth as the demographic dividend wanes and labor-cost advantages diminish. Politically, large language models and generative systems are seen as potential threats to the Party's information sovereignty. Consequently, the 2023 Generative AI Interim Measures mandate that AI outputs must "embody core socialist values" and require service providers to verify user identities and retain interaction logs for six months [6]. This extension of the Party's information control apparatus into the generative layer of the AI technology stack has substantial implications for both domestic innovation capabilities and international market competitiveness.

The relationship between the state and firms adds another layer of complexity. Companies like Baidu, Alibaba, and Tencent have been recognized as "AI champions" and tasked with developing national AI platforms within designated sectors. This approach affords them preferential access to government procurement, proprietary datasets, and regulatory guidance. However, it comes with the caveat of deep integration into state surveillance infrastructure and susceptibility to sudden political intervention, as illustrated by the regulatory actions taken against Didi, Alibaba, and other platform firms in 2021 [8].

2.2. The United States AI Regulatory Framework

The governance of AI in the United States has been marked by significant institutional inconsistency. Federal AI policy has largely relied on aspirational executive orders and voluntary frameworks instead of binding regulations. The 2019 American AI Initiative and the 2022 Blueprint for an AI Bill of Rights [9] outlined normative principles but lacked enforcement mechanisms. Executive Order 14110, issued by the Biden administration in October 2023, represented the most ambitious federal intervention to date, requiring developers of advanced AI models to share their safety test results with the government and instructing agencies to develop sector-specific standards [10]. However, the subsequent partial rescission of this order by the Trump administration in early 2025 underscores the policy volatility that is characteristic of the U.S. approach.

Congressional action has been notably limited. The lack of a comprehensive federal AI statute has resulted in a fragmented governance model, with oversight distributed among existing sector-specific regulators; the Federal Trade Commission (FTC) for consumer protection, the Securities and Exchange Commission (SEC) for financial services applications, and the Equal Employment Opportunity Commission (EEOC) for issues related to AI-driven hiring discrimination [11]. The AI Safety Institute, established within the National Institute of Standards and Technology (NIST), serves as a focal point for technical standard-setting, although it lacks regulatory authority. At the state level, California's AB 2013 and the ultimately vetoed SB 1047 represent proactive efforts highlighting both the absence of federal leadership and the increasing political relevance of AI-related risks [12].

A defining characteristic of the U.S. regulatory landscape is the federal government's structural dependence on private AI developers. The most advanced AI systems are created by private entities such as OpenAI, Google, DeepMind, Anthropic, and Meta, none of which operate under direct state ownership or mandates [13]. Currently, no federal agency possesses the necessary human capital or computational infrastructure to independently assess frontier AI systems. This asymmetry turns AI governance into a negotiation between regulators and those being regulated, systematically limiting the scope of obligations the government can credibly threaten to enforce.

3. In-Depth Examination of Institutional Friction Points

3.1. China: The Innovation-Control Paradox and Compliance Cost Asymmetry

China's AI governance framework presents a fundamental contradiction that remains unresolved within its current political economy. Authentic frontier AI research necessitates conditions such as open publication, international collaboration, academic freedom, and unpredictable exploratory inquiry, elements that the Party's information control apparatus actively suppresses [14]. The requirement for generative AI outputs to reflect "core socialist values" creates a competitive disadvantage in international markets, where users expect unrestricted utility. More critically, this mandate embeds censorship at the model level, forcing providers to modify systems in ways that compromise general capabilities in exchange for adhering to political content. Models like Alibaba's Qwen and Baidu's ERNIE illustrate this trade-off: while they perform competitively across various domains, they consistently exhibit evasion when dealing with politically sensitive topics during complex multi-turn interactions [15].

The compliance cost asymmetry is particularly pronounced for smaller entities. The Data Security Law and the Personal Information Protection Law (PIPL), both enacted in 2021, established a data governance framework that, when coupled with restrictions on cross-border transfers, significantly complicates international data partnerships essential to competitive model training [16]. Major AI incumbents can absorb these compliance costs through offshore subsidiaries, academic collaborations, and commercial licensing arrangements, mechanisms that often circumvent the regulatory intent while providing a veneer of legal protection. In contrast, smaller AI startups and academic research groups, lacking comparable compliance infrastructures and global networks, are unable to access these workarounds. The overall effect is a regulatory entrenchment of incumbent advantages disguised as data sovereignty protection.

At the macroeconomic level, the constraints on cross-border data flows impose a significant innovation tax. Research highlighting the productivity gains from international collaboration in AI, through co-authored publications, shared benchmarks, and open-source model development, indicates that the cumulative costs of China's data localization regime disproportionately impact the distributed, competitive, and sometimes disruptive innovation ecosystem that is essential for genuine technological leadership [17]. The primary beneficiaries of this misalignment are the Party apparatus, which maintains a mechanism of control, and large incumbent firms, which enjoy reduced competitive pressure. The burdens, in turn, are shouldered by smaller firms, academic researchers, and the broader aspiration for frontier capability development.

3.2. The United States: Fragmentation, Regulatory Vacuums, and Lobbying Dynamics

The governance challenges faced by the United States are structurally opposed to those encountered by China. While China enforces excessive centralization and uniformity on a fundamentally decentralized technology landscape, the United States grapples with regulatory fragmentation that makes coordination failures almost unavoidable. Executive Order 14110 set specific reporting thresholds for models trained with more than 10^{26} floating-point operations, which were deliberately calibrated to exempt most currently deployed systems [10]. This threshold, influenced by persistent lobbying from the technology sector, implies that the most significant provisions of the framework pertain to an exceedingly small subset of hypothetical future models rather than to the systems already causing real-world harms[18].

This sectoral regulatory framework gives rise to a particular form of governance failure known as cross-domain harms. For instance, an AI-driven mental health application that also serves as a financial advisor must navigate conflicting compliance obligations under FTC consumer protection rules, SEC financial regulations, and potentially EEOC employment guidelines. Yet there is no coordinating authority with a clear mandate to address the harms arising at the intersection of these domains. This regulatory vacuum is not simply an issue of implementation; it is a structural characteristic of a system designed to maintain maximum regulatory discretion at the industry level. As a result, firms can strategically design products that exploit jurisdictional ambiguities, leading to harms that fall outside the purview or incentive of any single regulator to address.

The political economy underlying this fragmentation is self-reinforcing. Technology firms have effectively reframed AI governance as an innovation policy issue rather than a public safety issue, portraying binding oversight as economically unpatriotic in the context of U.S.-China strategic competition [19]. This narrative has been internalized in Congress, as evidenced by the extensive testimony from AI developers during the Senate's 2023 hearings, which, however, resulted in minimal legislative output. Given that leading AI companies serve as significant campaign contributors and vital defense contractors, the political costs of imposing binding obligations are structurally amplified across administrations, regardless of partisan affiliation.

Moreover, the executive order mechanism poses a structural vulnerability. While executive orders have influenced U.S. AI policy in the absence of congressional action, they are inherently reversible, as demonstrated by the 2025 partial rescission of EO 14110. This instability creates a distinct compliance cost for the industry: firms struggle to make sustainable long-term investments when the regulatory landscape might shift dramatically after each election cycle. Paradoxically, this unpredictability benefits large incumbents, as they can absorb compliance uncertainty, while smaller entrants are disadvantaged, requiring predictable regulatory environments for effective investment planning.

3.3. Comparative Political-Economic Analysis

An examination of the two systems reveals that China's centralized model provides an enforcement speed that the U.S. system fundamentally cannot match. The Cyberspace Administration of China (CAC) can eliminate non-compliant AI applications from domestic platforms within hours, whereas comparable outcomes in the U.S. typically require years of litigation by the Federal Trade Commission (FTC) [20]. For specific, well-defined regulatory aims, such as preventing the dissemination of overtly harmful content, this speed differential offers a significant advantage. However, when it comes to governing something as dynamic, technically intricate, and context-sensitive as frontier AI systems, enforcement speed takes a back seat to regulatory wisdom. Unfortunately, the imperatives of Party information control undermine the effectiveness of the technical governance process.

The constitutional structure of the U.S. federal system imposes distinct constraints. The separation of powers requires durable AI legislation to garner legislative consensus—a task rendered nearly impossible by the current partisan climate. While executive orders can temporarily fill this legislative gap, they do so at the expense of long-term stability. Consequently, the regulatory environment becomes one in which neither the government nor the private sector can reliably commit to sustained long-term governance frameworks, fostering the very conditions that enable regulatory arbitrage to thrive [21].

In terms of achieving a balance between innovation and regulation, neither the Chinese nor the U.S. model succeeds effectively. China's system directs innovation towards state-favored sectors while systematically stifling disruptive inquiry that could threaten political authority. In contrast, the U.S. model promotes rapid innovation but overlooks social costs and fails to channel outcomes toward public goods. Both countries are advancing towards artificial intelligence capabilities that significantly exceed governmental understanding, with regulatory frameworks originally designed for a slower technological pace retroactively applied to systems with fundamentally different risk profiles [22].

A comparative analysis of the EU AI Act offers a valuable third perspective. The Act's risk-tiered classification, distinguishing between unacceptable-risk, high-risk, limited-risk, and minimal-risk applications, illustrates that binding horizontal AI legislation is politically feasible within democratic systems [23]. Furthermore, the Act's extraterritorial reach concerning systems deployed within the EU creates de facto global compliance pressures, contributing to what scholars refer to as a "Brussels Effect" in AI governance, similar to the impact of GDPR on global privacy standards [24]. In contrast, neither China nor the United States has developed a similarly coherent legislative framework, albeit for different reasons: China's prioritization of Party information control compromises technical governance, while the United States has faced industry lobbying that has effectively hindered the establishment of legislative consensus.

4. Policy Revision Proposals and Trade-Off Analysis

4.1. China: Disaggregating Information Control from Technical AI Governance

A significant and transformative reform for China would involve separating information control functions from the governance of technical AI systems. This could be accomplished by establishing a dedicated regulatory authority focused solely on technical aspects, distinct from the CAC's censorship responsibilities, and endowed with clear jurisdiction over AI safety, reliability, and market competition. By framing this initiative as a measure to enhance economic competitiveness—rather than a reduction in political oversight—it could increase its administrative viability. The impetus for this change is palpable: the growing skepticism in international markets toward Chinese AI products, rooted in concerns about political constraints, poses a tangible economic challenge that policymakers can quantify and acknowledge as a strategic liability.

The trade-offs are significant and must be recognized. Establishing a technically autonomous AI regulatory body would necessitate the Communist Party to accept a meaningful reduction in its operational control over commercial AI systems. Even if presented as an economic imperative, this represents a structural concession that the Party's current political framework is ill-suited to accommodate. A more politically viable initial step could be an intermediate reform: creating a technical advisory panel with non-binding authority to recommend adjustments to content mandate thresholds. This approach could set an institutional precedent for expert autonomy within the existing governance structure.

4.2. United States: Federal AI Act and Unified Regulatory Authority

In the United States, a key priority for reform is the enactment of a comprehensive federal AI Act that establishes a unified regulatory authority equipped with technical expertise, enforcement capabilities, and a clear cross-sectoral mandate for high-risk AI applications. The risk-tiered framework of the EU AI Act serves as a legislative blueprint; however, the primary challenge lies in adapting it to the U.S. constitutional context while ensuring the regulatory body has adequate technical capacity to evaluate advanced AI systems [23]. Crucially, the issue of reporting thresholds identified in Executive Order 14110 must be resolved. These thresholds should be defined based on application risk category and deployment scale, rather than solely on training compute, to ensure that high-impact systems currently in use are effectively covered.

The economic trade-offs associated with this approach require careful consideration. A unified regulatory mandate may impose compliance costs on smaller AI developers that are disproportionate to their market power, potentially leading to further concentration within the industry around well-resourced incumbents. Therefore, regulatory design should incorporate tiered compliance obligations calibrated to firm size and deployment scale, coupled with expedited pathways for smaller developers working in lower-risk application categories. The alternative, continued regulatory fragmentation, carries its own economic costs due to compliance uncertainty, cross-jurisdictional inconsistencies, and the systemic underpricing of AI-related risks, which will ultimately manifest as public harm.

4.3. Emerging Markets: Regional Coalitions and the Infrastructure Cost Dimension

Nations in Southeast Asia, Sub-Saharan Africa, and Latin America grapple with a fundamental dilemma: they possess insufficient regulatory capacity for independent AI governance while simultaneously facing the extraterritorial consequences of governance decisions made in Beijing and Washington [25]. Embracing China's model necessitates acceptance of political content restrictions and integration into a surveillance infrastructure known for its ability to suppress civil society. Conversely, adopting the U.S. model results in regulatory fragmentation and reliance on platforms managed by entities whose commercial motivations are often misaligned with national development objectives.

A critical economic trade-off that has not been adequately addressed in earlier analyses is the infrastructure dimension related to data governance choices. Stringent data localization policies, similar to those outlined in China's PIPL, impose

considerable infrastructure costs on emerging economies. These costs include the construction of domestic data centers, the establishment of localized cloud infrastructures, and the development of specialized compliance capacities that many low- and middle-income countries simply cannot afford without sacrificing other crucial development priorities [26]. On the other hand, permissive data governance frameworks leave domestic consumer data exposed to extraction by foreign technology platforms, creating a form of digital colonialism in which local data generates value entirely captured outside the national economy.

A more sustainable approach entails establishing regional regulatory coalitions, through organizations such as the African Union, ASEAN, MERCOSUR, or similar entities, to formulate shared standards that maintain domestic policy autonomy while ensuring interoperability with major AI ecosystems. These coalitions could implement risk-tiered frameworks, similar to the EU AI Act, at the regional level, leveraging collective bargaining power to negotiate data governance terms with platform providers. Successful execution of this strategy would require ongoing technical assistance from multilateral institutions such as UNCTAD, the ITU, and the World Bank, as well as proactive support from countries with established governance infrastructures. A critical success factor is that these frameworks must authentically reflect regional development priorities, such as infrastructure cost constraints and digital sovereignty objectives, rather than merely replicating governance models intended for high-income economies with fundamentally different institutional and resource contexts.

5. Conclusion

This comparative analysis demonstrates that we are not witnessing a contest between a functional and a dysfunctional AI governance system, but rather two frameworks whose failure modes are inherently tied to their respective political economies. In China, the Party-state struggles to govern AI effectively because the imperatives of information control fundamentally compromise the technical governance process. In the United States, the fragmented, market-driven approach fails to govern AI effectively due to a lack of institutional coherence and political resolve needed to impose significant obligations on the firms it relies upon. Both nations have developed regulatory architectures that primarily benefit established actors, state-affiliated champions in China, and leading model developers in the United States, while systematically shifting costs onto those without the political leverage to impact regulatory design.

These failure modes highlight deeper tensions within each nation's political structure: in China, the conflict between the Party's legitimacy claims and the prerequisites for genuine technological excellence; in the United States, the tension between democratic capitalism's tolerance for private power and the public-interest demands posed by transformative technology. Recognizing these tensions makes it clear that AI governance is not merely a technocratic issue waiting for the appropriate policy instrument. It is fundamentally a political challenge that necessitates engagement with questions of sovereignty, legitimacy, and power distribution, issues that no amount of technical standard-setting can adequately address.

The broader implications for global technology governance are significant. A landscape where AI standard-setting is contested between two powers, each with internally contradictory governance models, is likely to lead to fragmentation, regulatory arbitrage, and ongoing accountability gaps regarding AI-related harms. Achieving progress necessitates not only enhancements in national regulation but also the creation of new international governance institutions capable of establishing binding standards on the cutting edge, institutions that require both China and the United States to accept constraints on their AI sectors, which their current political frameworks are structurally ill-equipped to accommodate. This challenge, the political willingness to accept externally binding obligations, remains the most critical and inadequately addressed issue in contemporary AI governance.

Compliance with ethical standards

Acknowledgments

The author expresses gratitude for the valuable feedback received from the Department of Information Technology, School of Computer and Information Science, University of the Cumberlands. This study was conducted without any external funding.

Disclosure of conflict of interest

The author hereby declares that there are no conflicts of interest, whether financial or otherwise, associated with this manuscript.

References

[1] Dafoe, A. (2018). AI Governance: A Research Agenda. Center for the Governance of AI, Future of Humanity Institute, University of Oxford. Available from: https://www.fhi.ox.ac.uk/wp-content/uploads/AI-Governance-Research-Agenda.pdf

[2] Brantly, A.F. (2017). The cyber dimension of the Chinese National Security Strategy. Orbis, 61(2), 187–204.

[3] Coglianese, C., & Lehr, D. (2017). Regulating by robot: Administrative decision-making in the machine-learning era. Georgetown Law Journal, 105(5), 1147–1223.

[4] Ang, Y.Y. (2020). China's Gilded Age: The Paradox of Economic Boom and Vast Corruption. Cambridge: Cambridge University Press.

[5] State Council of the People's Republic of China. (2017). Notice of the State Council issuing the new generation of artificial intelligence development plan. Beijing: State Council.

[6] Cyberspace Administration of China. (2023). Interim measures for the management of generative artificial intelligence services. Beijing: CAC.

[7] Webster, G., Creemers, R., Triolo, P., & Kania, E. (2017). China's plan to 'lead' in AI: Purpose, prospects, and problems. New America. Available from: https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/

[8] Greitens, S.C. (2020). Surveillance, security, and liberal legibility: The social and political conditions of surveillance technology. Perspectives on Politics, 18(4), 1091–1107.

[9] White House Office of Science and Technology Policy. (2022). Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. Washington, DC: The White House.

[10] Executive Office of the President. (2023). Executive Order 14110: Safe, secure, and trustworthy development and use of artificial intelligence. Federal Register, 88(210), 75191–75226.

[11] Marchetti, C. (2023). Emerging regulatory approaches to artificial intelligence. Journal of Internet Law, 27(1), 3–18.

[12] Reisman, D., Schultz, J., Crawford, K., & Whittaker, M. (2018). Algorithmic impact assessments: A practical framework for public agency accountability. AI Now Institute. Available from: https://ainowinstitute.org/aiareport2018.pdf

[13] West, S.M. (2022). Redistribution and rekindling: AI policy proposals and the specter of automation. AI & Society, 37(4), 1379–1392.

[14] Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation. AI & Society, 36(1), 59–77.

[15] Stanford Human-Centered Artificial Intelligence. (2024). AI Index Report 2024. Stanford, CA: Stanford University. Available from: https://aiindex.stanford.edu/report/

[16] Greenleaf, G. (2021). China's new Personal Information Protection Law: Comparisons with GDPR. Privacy Laws & Business International Report, (174), 1–7.

[17] Arora, S., & Arora, P. (2022). Artificial intelligence and international scientific collaboration: Bibliometric evidence and policy implications. Research Policy, 51(1), 104404.

[18] Bommasani, R., Klyman, K., Zhang, D., & Liang, P. (2023). Do foundation model providers comply with the EU AI Act? Stanford CRFM Technical Report. Available from: https://crfm.stanford.edu/2023/06/15/eu-ai-act.html

[19] Runciman, D. (2018). How Democracy Ends. London: Profile Books.

[20] Marchetti, C., & Bertolini, L. (2022). Artificial intelligence regulation: A framework for governance. European Journal of Risk Regulation, 13(2), 198–218.

[21] Coglianese, C. (2021). Artificial intelligence and regulatory capacity. Journal of Regulation, 3(1), 17–28.

[22] Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. UC Davis Law Review, 51(2), 399–435.

[23] European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union

[24] Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. New York: Oxford University Press.

[25] Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': The US, EU, and UK approach. Science and Engineering Ethics, 24(2), 505–528.

[26] Ndemo, B., & Weiss, T. (Eds.). (2017). Digital Kenya: An Entrepreneurial Revolution in the Making. London: Palgrave Macmillan.