ARTICLE

Governing Artificial Intelligence: Comparing AI Regulation among BRICS

HELDER FERREIRA DO VALE

Federal University of Bahia, Brazil

ORCID No: 0000-0002-4993-7932

ABSTRACT *The article examines AI regulation in BRICS countries through a typology of AI regulatory governance and a BRICS AI Readiness Index. Based on these analytical tools, the article assesses ethical, economic, governance, and temporal factors that influence the regulatory readiness of the five BRICS. This index mainly draws from a qualitative assessment of national legislation and AI national strategies. Based on this index, the article finds China the most prepared of the BRICS to regulate AI deployment, while Brazil, India, and South Africa show promises but face challenges in developing regulations. Russia appears in the Index as a clear laggard in the adoption of an AI regulatory framework. The article highlights ethical trade-offs, the complex relationship between public trust and regime type, and the relevance of temporal parameters to regulating AI. It calls for tailored policies to strengthen AI governance across BRICS countries.*

Keywords: AI, Regulation, BRICS, Index, Governance

Insight Turkey 2025
Vol. 27 / No. 2 / pp. 337-364

Received Date: 12/5/2025 • **Accepted Date:** 26/6/2025 • **DOI:** 10.25253/99.2025272.18

Introduction

As artificial intelligence (AI) continues to advance rapidly, the need for proactive policy responses becomes increasingly necessary. Divergent predictive models on AI's future reveal a lack of consensus,[1] underscoring a critical problem: while rapid technological progress risks outpacing existing policies, regulatory inaction is equally untenable in the face of potential superintelligence risks. This highlights the urgent need to evaluate and enhance the regulatory readiness of countries.

AI technologies present a range of pressing challenges, including job displacement, algorithmic bias, and rising economic inequality. In this context, the role of Global South countries in AI governance is coming under growing scrutiny, as these countries are gaining greater relevance in shaping global order. Particularly, as the alliance between Brazil, Russia, India, China and South Africa (BRICS) reassures its global status as a critical player in global governance, it is important to understand the regulatory capacity of these countries.

This article analyzes BRICS national AI strategies, exploring the potential and limitations for Global South countries governing AI to harness its development benefits while mitigating disruption. Key measures include enacting flexible, innovation-friendly regulations, establishing dedicated AI governance agencies, and promoting regional cooperation.[2] Geopolitically, while AI development is superpower-dominated, China's cooperative posture toward the Global South, including technology transfer, could decentralize innovation and support international regulatory frameworks. Proposals even suggest a global AI governance body, similar to the European Council of Nuclear Research (CERN), to coordinate efforts and prevent power imbalances through inclusive collaboration. The trajectory of five BRICS' countries is analyzed here to extract important lessons that are valuable to the development of a regulatory framework for Global South countries. Specific policy tools in each country are relevant to drawing policy recommendations and conclusions for the future development of AI beyond high-income countries.

China's technological dominance strengthens its influence within the BRICS, but others may pressure it to balance prosperity with equity. Variation among BRICS rules, concepts, and principles in AI adoption requires an examination of the main regulatory patterns within BRICS. In doing so, this article develops a typology based on geopolitical and civilian AI use and introduces the AI Readiness Index, which assesses each country's capacity, across ethical, economic, governance, and temporal dimensions, to regulate AI effectively. The index frames readiness as a holistic ability to manage AI's risks, complexities, and opportunities for sustainable development within the BRICS context.

This article has seven sections. In the next section, it introduces a framework and typology to classify BRICS countries in terms of AI regulation. In section three, it analyzes their regulatory contexts and defines four key dimensions for assessing the BRICS AI Readiness Index. Section five details the indicators used for measurement, while section six discusses the findings. Section seven concludes with policy recommendations to enhance AI regulatory readiness across BRICS countries.

Geopolitically, while AI development is superpower-dominated, China's cooperative posture toward the Global South, including technology transfer, could decentralize innovation and support international regulatory frameworks

General Framework on AI Technology

The convergence of military and civilian AI use, known as AI dual-use, raises serious global governance concerns.[3] AI's application in surveillance may erode democratic values and enable authoritarianism,[4] although it also holds the potential for enhancing civic participation if responsibly managed.[5] Scholars stress the need for AI regulation to incorporate ethical and sovereignty issues, not just economic ones.[6] Without strong oversight, tech firms may amass excessive influence.[7] To navigate into these different types of regulatory factors, this article proposes a typology to guide our analysis of BRICS.

The typology introduced here divides AI usage into two broad axes: Geopolitical-Security Application and Civilian-Commercial Application. Each category necessitates unique regulatory strategies to harmonize innovation, security, and ethical principles. The different degrees of application of AI technology produce four different regulatory types: Laissez-Faire Governance, Authoritarian Control, Democratic Governance, and Capable Hybrid Control.

The Geopolitical-Security Application Axis indicates the extent to which a country advances and utilizes AI for strategic governmental objectives. This encompasses military benefits, including enhanced surveillance, automation, and cyber capabilities through complex systems (e.g., Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance – C4ISR) that augment state authority via military surveillance systems and autonomous weaponry (e.g., Lethal Autonomous Weapons – LAWS). There are different patterns of AI military use that can be used in different combinations, making AI capability adaptable to various purposes: goal-driven systems for autonomous drones, autonomous systems such as self-driving military vehi-

Democracies are more inclined to endorse high levels of civilian AI utilization, fostering innovation and accessibility. Conversely, authoritarian regimes may limit civilian uses of AI, favoring control over empowerment

cles, conversational interactions for military communication, predictive analytics and decisions for military equipment, hyperpersonalization to make technology and equipment personalized, AI decision support for decision-making in military operations, and recognition patterns for military surveillance.[8]

The Civilian-Commercial Application Axis delineates the extent of AI integration inside governmental and private sectors for non-security purposes. This encompasses applications in health, education, and public services, as well as consumer technologies. This can be quantified by evaluating the market penetration of AI products, private research and development spending, and the integration of AI in public administration for non-enforcement applications. Democracies are more inclined to endorse high levels of civilian AI utilization, fostering innovation and accessibility. Conversely, authoritarian regimes may limit civilian uses of AI, favoring control over empowerment.

Figure 1 depicts the four types of AI regulatory governance. It is essential to note that distinguishing between military and civilian applications of AI is becoming increasingly challenging, as models designed for civilian purposes (e.g., Large Language Models – LLM) can support military AI systems (e.g., C4ISR).[9] This typology, despite its thin boundaries, provides a framework for investigating the different dimensions of AI regulation.

Figure 1: Typology of Regulatory Governance for AI

		GEOPOLITICAL-SECURITY APPLICATION	
		Low	High
CIVILIAN-COMMERCIAL APPLICATION	Low	Quadrant 1 *Laissez-Faire Governance*	Quadrant 2 *Authoritarian Control*
	High	Quadrant 3 *Democratic Governance*	Quadrant 4 *Capable Hybrid Control*

Source: *Author's own elaboration*

Quadrant 1: Laissez-Faire Governance (Low Geopolitical-Security Application, Low Civilian-Commercial AI)
This regulatory environment emerges when AI applications have minimal strategic military value and limited civilian penetration. Such conditions create fertile ground for unconstrained AI experimentation and fundamental research. Characterized by light-touch regulation, this approach deliberately minimizes state intervention to stimulate innovation and attract investment. The regulatory framework typically relies on voluntary ethical guidelines rather than binding legislation, while consciously avoiding antitrust measures that might constrain development. This hands-off approach stems from the recognition that premature or excessive regulation could impede foundational breakthroughs in AI domains.

Quadrant 2: Authoritarian Control (High Geopolitical-Security Application, Low Civilian-Commercial AI)
This regulatory context represents a regulatory imbalance in which AI development becomes overwhelmingly dominated by military and security priorities at the expense of civilian applications. This governance model systematically prioritizes the interests of defense establishments and political elites over transparent, accountable AI deployment. Regulatory mechanisms in such a context focus mainly on enhancing state power through military surveillance systems and autonomous weapons. The inherent opacity of such programs creates a self-reinforcing cycle: as AI militarization advances without public oversight, authoritarian tendencies intensify, further eroding democratic checks and balances in technological development.

Quadrant 3: Democratic Governance (Low Geopolitical-Security Application, High Civilian-Commercial AI)
This regulatory framework governs AI systems that primarily serve social and economic needs rather than security objectives, encompassing consumer technologies such as transformative tools in healthcare and education. The regulatory approach under this framework can be understood under Thumfart's concept of "democratic offset," which suggests that institutionalizing robust public participation in AI governance may offset the negative effects of AI deployment.[10] Market regulation plays a crucial role in preventing corporate monopolies while ensuring fair competition. By embedding democratic values into AI systems that touch citizens' daily lives, this model aligns technological development with societal expectations and fundamental rights.

Quadrant 4: Capable Hybrid Oversight (High Geopolitical-Security Application, High Civilian-Commercial AI)
The most complex regulatory challenge emerges when AI technologies possess significant dual-use potential, simultaneously serving civilians and military/security functions. This context demands a sophisticated governance appara-

tus capable of enforcing corporate accountability through mandatory ethical audits while implementing rigorous national security safeguards such as export controls and adversarial testing. The regulatory framework must address the inherent tensions between innovation incentives and risk mitigation, developing mechanisms to distinguish between legitimate civilian applications and potential military misuse. This hybrid model represents the cutting edge of AI governance, requiring constant adaptation to address evolving technological capabilities and geopolitical realities. An example of this advancement combining different facets of military intelligence and technology is AI-enhanced C4ISR systems.

Applying the four regulatory frameworks to BRICS, China stands alone in Quadrant 4, combining civilian AI leadership with significant militarization, reflecting its global ambitions. No BRICS country fits Quadrant 1, as no country adopts laissez-faire approaches in strategic sectors. Brazil, India, and South Africa align with Quadrant 3, emphasizing democratic governance and civilian AI use, though Brazil and India face growing dual-use risks and seek greater geopolitical influence. South Africa maintains a civilian focus but it has limited technological penetration and modest global leverage. Russia falls into Quadrant 2, prioritizing military AI with minimal civilian applications but significant geopolitical influence.

Regulatory Framework

Democratic Governance

Brazil and India have established AI regulations reflecting domestic priorities, while South Africa is still drafting its rules. Brazil, India, and South Africa share similarities within BRICS AI regulation: viewing AI as risky, incorporating ethical/democratic principles, and facing funding constraints hindering hub aspirations. However, Brazil differs significantly. It lacks specific AI sandbox regulations (unlike India and South Africa); employs a centralized oversight body (versus fragmented oversight elsewhere); and focuses regulations primarily on public sector AI, while the others regulate both public and private sector AI.

Brazil's Algorithmic Accountability Bill (PL 21/2020) mandates transparency for public-sector AI, bans high-risk policing AI without judicial approval, and imposes civil liability for algorithmic discrimination.[11] While enhancing public accountability, it excludes the private sector, allowing commercial AI development to proceed largely unregulated. This creates a regulatory gap, giving private actors a market advantage. In December 2024, Brazil's Senate approved the AI Law (2.338/2023),[12] now under review in the lower house. Inspired by the European Union AI Act, it mandates human oversight, transparency, fair-

ness, and a risk-based approach to AI regulation.

Brazil, India, and South Africa share similarities within BRICS AI regulation: viewing AI as risky, incorporating ethical/democratic principles, and facing funding constraints hindering hub aspirations

Brazil is comparatively advanced in AI regulation within Latin America, but its National Data Protection Authority (ANPD) still lacks the resources to effectively audit AI systems. Until recently, the country lacked a formal AI strategy.[13] However, the launch of the Brazilian Artificial Intelligence Plan (PBIA 2024-2028) represents major progress. With BRL 23 billion ($4 billion) in projected investments in innovation, infrastructure, and training, Brazil is now better positioned to meet the regulatory challenges of emerging AI technologies.[14]

The proposed Digital India Act (DIA) will adopt a risk-based approach to AI regulation, targeting harmful applications like deepfakes and high-risk sectors such as healthcare.[15] It differentiates rules based on company size, eases compliance for startups, and requires government-run AI systems to offer open APIs. Praised for avoiding over-centralization, it complements the IndiaAI Mission, which promotes a national AI ecosystem. A key achievement is the creation of the Safety Institute for Responsible AI Innovation to foster cross-sector collaboration, in a context where oversight is fragmented.

Despite strong technical talent, the sector is underfunded. Critics argue that exempting startups could be dangerous, as advanced AI might emerge from small labs. There are also concerns that India focuses too much on harmful outputs rather than systemic risks. Experts urge the redirection of India's tech talent toward AI alignment research. India would also benefit from harmonizing its approach with ASEAN's AI governance efforts.

South Africa is developing its comprehensive AI legislation under the National AI Policy Framework,[16] which draws from international best practices and aligns closely with the EU's model. The framework emphasizes ethics, social equity, and economic growth while addressing risks such as technological misuse, job displacement, and falling behind in global AI development. South Africa's existing data protection laws, the 2013 Protection of Personal Information Act (POPIA)[17] and the 2020 Cybercrimes Act,[18] support transparency, suggesting a solid foundation for a strong AI regulatory framework.

Nonetheless, the country faces significant challenges, including limited human capital, financial constraints, and regulatory fragmentation. The AI sector currently relies heavily on foreign funding and expertise. Establishing a

AI has provided the opportunity for Russia to close the military gap with the West by using unnamed automated vehicles, loitering munitions, and strategic decision-making

centralized regulatory authority is critical in South Africa, as current oversight is fragmented. For example, the Financial Sector Conduct Authority (FSCA) oversees financial AI, while the South African Health Products Regulatory Authority (SAHPRA) manages AI in healthcare.[19]

Authoritarian Control

Russia's AI regulation aligns with its geopolitical strategy, prioritizing military over civilian uses. This militarized focus drives centralized control of AI development within the country's regulatory framework. Russia's AI regulations are grounded in Presidential Decree No. 490 (2019),[20] issued by President Vladimir Putin, emphasizing strong state control. The decree adopts a risk-based approach, viewing AI as crucial for economic growth and military power. It also incorporates nationalist measures, restricting foreign access to AI technologies to safeguard Russia's technological sovereignty and strategic autonomy.

In line with these objectives, Russia introduced a flexible regulatory mechanism through Law No. 258-FZ (2020).[21] This law enables the creation of sandboxes' specific provisions. The sandbox approach reflects Russia's recognition of the need to innovate while maintaining strict oversight and national control over emerging technologies. Russia's National Strategy for AI Development until 2030 looks promising, especially concerning sandbox experimentation.

Overall, Russia's approach to AI regulation is deeply centralized and security-driven.[22] The *Roskomnadzor* tightly controls data and security information, and there is a need for the institution to be more transparent and accountable, while the mandate of the regulator should not be mixed with internet censorship.[23] It prioritizes national interests, strategic autonomy, and military advancement over civilian or democratic oversight, positioning AI as a critical tool in its pursuit of geopolitical influence. This is felt in the military realm through Russian advancement of electronic warfare systems.[24] AI has provided the opportunity for Russia to close the military gap with the West by using unnamed automated vehicles, loitering munitions, and strategic decision-making.[25]

Capable Hybrid Oversight

China governs AI to advance national interests, balancing innovation with strict regulation. AI serves as both an economic engine and a tool for social control. In 2021, China enacted two legislations: the Data Security Law

(DSL),[26] which manages data risks and storage, and the Personal Information Protection Law (PIPL),[27] which restricts facial recognition, algorithmic profiling, and enhances personal data protection across public and private sectors, forming the foundation of China's AI regulatory framework.

In 2023, China adopted the Generative AI Measures to regulate AI development and use,[28] followed in 2024 by the New Era AI Ethics Guidelines, emphasizing human well-being and ethical innovation.[29] AI governance is shared between the Cyberspace Administration of China (CAC), which approves public-facing systems, and the Ministry of Industry and Information Technology (MIIT), responsible for industrial standards. While the government promotes AI in strategic sectors such as manufacturing and healthcare, tight controls limit civilian access. AI use often requires a national ID, and reports indicate a "blacklist" restricting some users services.[30] Additionally, enforcement of national AI regulations varies across provinces, with significant inconsistencies in local implementation.[31] This regulatory framework reflects China's effort to balance technological advancement, ethical concerns, and centralized control over AI deployment.

China is actively enhancing its military capabilities through the development of the "systems of systems," namely, the C4ISR system, which the U.S. has identified as a significant strategic threat.[32] In the realm of Lethal Autonomous Weapons Systems (LAWS), China's stance remains ambiguous: while it publicly supports a legal ban on such weapons, it simultaneously advances their development and has declined to sign the United Nations Convention on Certain Conventional Weapons (CCW).[33]

While China continues to advance as a global AI power, its regulatory model reflects a balance between innovation and control, one that prioritizes state authority and security while cautiously expanding AI's societal applications. As a result, China is consolidating as a clear leader in infrastructure, innovation and regulation for AI deployment in the Global South.

The Four AI Dimensions

Temporal Dimension

Temporality plays an increasingly central role in how we understand the nature of artificial intelligence. AI operates across multiple temporal modalities: its rapid internal computational processes, its gradual but transformative impact on society, and its consequences on the persistent disparity between the rapid advancement of AI technology and the more measured pace of regulatory action. This threefold tension highlights the need for frameworks that align AI's acceleration with human and institutional timescales.



The 16th BRICS Summit was held in Kazan, Russia, on October 24, 2024, with the participation of more than 30 countries, including BRICS member states, partner countries, and invited observers.

IRANIAN PRESIDENCY / AA

The rapid evolution of AI often collides with slower human temporal frameworks, generating ethical and normative challenges. ChatGPT's swift deployment (2022-2023) outpaced regulations on copyright and disinformation, prompting reactive adjustments like the EU's AI Act revisions. As AI accelerates, it reshapes human experiences through its speed, duration, and frequency,[34] potentially altering how society perceives time. Governance must account for temporality although some warn that adaptive governance risks enabling "ethics washing" if led by corporate interests.[35]

As AI capabilities advance, they generate ethical challenges that quickly outdate existing guidelines,[36] requiring regulatory frameworks to be both anticipatory and adaptable. AI also raises questions about how it processes time, needing to reason about causality and event sequencing to function in human systems.[37] AI's development is shaped by both technical progress and public perception.[38] Its rapid learning and optimization profoundly influences deployment, human interaction, and broader societal impact.[39]

Ethical Dimension

As AI transforms society, ethical concerns regarding fairness, transparency, accountability, and value alignment become central. AI integration into everyday life is not merely a technical endeavor, but a fundamentally ethical one. This article explores how BRICS countries embed values and principles into their AI governance, addressing the distribution of responsibility within their regulatory and ethical frameworks.

Regulatory efforts must confront the challenge of algorithmic accountability, particularly through mechanisms such as algorithmic audits grounded in fairness and transparency, despite the difficulty of auditing complex systems.[40] Holding AI systems accountable requires more than legal oversight; it also demands an ethical framework that addresses the so-called "responsibility gap," the difficulty in attributing moral responsibility to the actions of non-human agents.[41]

An important challenge in AI governance is the increasing overlap between military and civilian AI applications. National security concerns can influence domestic policy, risking autocratic drift

A pluralistic approach to AI ethics supports diverse strategies for aligning AI with human moral expectations. Some focus on training AI to interpret data based on human needs,[42] while others emphasize embedding ethical principles through robust value alignment.[43] Yet, some question whether AI could develop ethical frameworks independent of humans,[44] enabling "ethics by design" systems.[45] Concepts such as the "ethics of AI belief"[46] and "morally autonomous systems" support this view.[47] However, some argue AI remains an extension of its creators' values.[48] This discussion becomes heatedly debated when dealing with LAWS, which has destructive power with AI systems.[49]

Despite the ongoing debate over how best to impose ethical constraints on AI, there is growing consensus in the literature on the necessity of establishing boundaries to prevent harm and ensure justice, transparency, and responsible governance.[50] In high-stakes sectors related to healthcare and criminal justice, ethical benchmarks are increasingly being introduced to evaluate AI's alignment with human values and social norms.[51]

Governance Dimension

AI governance involves formal regulations and informal norms such as public trust. However, fragmented reactive approaches to regulation hinder coherent national strategies, as research remains divided between empirical analysis and normative debate.[52]

In the realm of public management, while AI ideally calls for a decentralized and adaptive governance model,[53] prevailing regulatory responses tend to favor centralized control and top-down coordination. This paradox contributes to persistent fragmentation across sectors and technologies, impeding regulatory consistency.[54]

An important challenge in AI governance is the increasing overlap between military and civilian AI applications. National security concerns can influ-

Unlike previous technological revolutions, current projections suggest that white-collar and professional sectors, traditionally considered more resilient, may be disproportionately affected by advancements in AI

ence domestic policy, risking autocratic drift.[55] Some scholars advocate "forward-looking governance"[56] and strengthening democratic institutions with civic participation[57] to mitigate AI's potential negative impacts.

AI can improve service personalization and fairness if aligned with public interest.[58] However, system opacity undermines trust; 67 percent distrust government AI use due to transparency concerns,[59] deepening legitimacy gaps.

Economic Dimension

AI offers both opportunities and risks, including job displacement and rising inequality. However, with thoughtful governance, AI can drive inclusive, sustainable economic growth through innovation and enhanced productivity instead of exacerbating disparities or destabilizing labor markets and global economies.

AI's dual role, enhancing productivity while risking job loss and inequality, reflects the "productivity paradox."[60] This tension complicates regulatory efforts aimed at translating AI-driven gains into broadly shared prosperity. If this paradox continues unchecked, it may reinforce winner-takes-all dynamics, further concentrating economic power and exacerbating socioeconomic vulnerabilities.

Scholars propose redistributive measures such as Universal Basic Income (UBI) to counter AI-driven job loss.[61] Furthermore, proposals suggest tax reforms, expanded social protections, and workforce retraining to address AI's labor impact,[62] although some argue deeper economic paradigm shifts are needed.[63]

Unlike previous technological revolutions, current projections suggest that white-collar and professional sectors, traditionally considered more resilient, may be disproportionately affected by advancements in AI.[64] This signals a departure from historical patterns of labor disruption and underscores the need for proactive and adaptive policy responses to safeguard economic equity.

Measurement

The measurement of variables is based on a qualitative assessment of legal, institutional, and contextual factors, which will be detailed for each country. Each variable is scored on a scale from 1 to 5, where 1 indicates a low level of readiness and 5 reflects a high level.

As previously outlined, the assessment is structured around four key dimensions: ethical, governance, economic, and temporal. Each dimension comprises specific variables and indicators, which collectively contribute to evaluating a country's readiness to regulate artificial intelligence.

The results are presented in Table 1, which displays the AI Readiness Index for each country. Among the BRICS countries, China emerges as the most prepared to regulate AI, followed closely by Brazil, India, and South Africa. The differences between these four countries are relatively minor. Russia, however, lags significantly behind, marking a notable gap in readiness.

The democratic triad, Brazil, India, and South Africa, demonstrates promising regulatory potential, despite facing challenges in certain areas. Brazil stands out for its balanced performance across all four dimensions, with variation not exceeding 1 points. In contrast, India and South Africa each exhibit a lag in at least two specific dimensions.

Table 1: BRICS AI Readiness Index

	Ethics Dimension	Economic Dimension	Governance Dimension	Temporal Dimension	AI Readiness Index
China	3	4.3	3.3	5	**3.9**
Brazil	3.5	3.0	4	3	**3.3**
India	2.5	3.3	3.3	4	**3.2**
South Africa	2.5	2.3	3.6	4	**3.1**
Russia	1	2	2	1	**1.5**

Source: *Author's Own Elaboration*

Ethical Variables

The ethical dimension is assessed through two variables: value alignment and algorithmic accountability. The evaluation of these variables draws from the available literature on each country's legislation and regulatory efforts concerning these issues. Yet, the OECD's human value benchmark, based on five clusters, inclusive growth, sustainable development and well-being; human rights and democratic values; transparency and explainability; robustness, security and safety; and accountability, has been used to assess the legislation of countries.[65]

The results suggest a modest trade-off between value alignment and accountability: Brazil aligns with public values but struggles with enforcement, while China enforces audits but neglects value integration. Though based on textual

analysis, the study includes real-world systems like India's Aadhaar and China's Social Credit, highlighting their impact on rural access to services.

As shown in Table 2, Brazil ranks highly on ethical indicators, particularly excelling in value alignment. Russia, by contrast, shows the weakest performance in this dimension. India and South Africa score similarly, with stronger results in value alignment than in algorithmic accountability. China's overall performance is comparable to that of India and South Africa, although it places greater emphasis on algorithmic accountability at the expense of value alignment.

Table 2: Measurement of Ethics Variables

Country	Value Alignment (V.A.)	Algorithmic Accountability (A.A.)	Total *(average)*	Key Supporting Data
China	3	3	**3**	**V.A.:** Top-down "socialist values" alignment; Corporate self-governance (e.g., Alibaba) **A.A.:** Domestic auditing standards (e.g., 2023 AI rules); No transparency for state AI; Global export of surveillance tech
Brazil	4	3	**3.5**	**V.A.:** Strong legal frameworks (LGPD, AI Bill); Equity-focused discourse; Limited rural inclusion **A.A.:** Algorithmic transparency laws (e.g., São Paulo's facial recognition ban); Weak enforcement outside cities
India	3	2	**2.5**	**V.A.:** "AI for All" rhetoric; Civil society pushes for rights; Tech industry self-regulation **A.A.:** No mandatory audits; Aadhaar shows accountability gaps; Draft Digital India Bill pending
Russia	1	1	**1**	**V.A.:** AI ethics subordinated to state security; No public input; Symbolic "Ethics Charter" **A.A.:** No independent oversight; Military AI exempt from scrutiny; Siloed development
South Africa	3	2	**2.5**	**V.A.:** Emerging *Ubuntu*-inspired ethics; Healthcare AI equity focus; Limited policy formalization **A.A.:** No algorithmic liability laws; Private sector unregulated; Pilot projects (e.g., TB diagnostics)

***Value Alignment**: 5 = High ethical standard (five OECD clusters), 4 = Moderate ethical standards (four OECD clusters), 3 = Moderate-ethical standards (two OECD clusters), 2 = Low ethical standards (one OECD cluster), 1 = No clear ethical standards. Source: Country's legal text.*[66]
***Algorithmic Accountability**: 5 = Specific legislation on the matter with auditing capability, 4 = Specific legislation on the matter with limited auditing capability, 3 = Specific legislation with no mandatory audit; 2 = No specific legislation but some audits or oversight, 1 = No specific legislation and no mandatory audits. Source: Country's legal text.*[67]

Economic Variables

The economic dimension of AI readiness is evaluated through three variables: digital infrastructure, ecosystem for innovation and quality for innovation. These variables represent foundational elements for technological advancement and reflect the depth of AI integration into a country's economic system.

Brazil and Russia both demonstrate potential for AI development but face distinct obstacles, such as regional disparities in Brazil and international sanctions affecting Russia

To assess these variables across the BRICS countries, digital infrastructure was measured using 5G penetration. The innovation ecosystem was assessed based on the incentive structure for patents measured by the total number of patents per capita. The quality of innovation, which is often associated with the registration of new patents, reflects the existence of proper incentives for technological progress. Although assessing patent quality is complex,[68] a simple proxy involves examining national registration requirements to process patents.

Overall, China clearly leads in the economic dimension. India shows significant potential but requires greater investment in digital infrastructure. South Africa lags behind due to systemic challenges, including limited infrastructure and insufficient funding. Brazil and Russia both demonstrate potential for AI development but face distinct obstacles, such as regional disparities in Brazil and international sanctions affecting Russia.

In terms of digital infrastructure, China stands out as a global leader, with widespread 5G deployment. India falls into the high-moderate range with a rapid rollout of 5G in urban centers. Brazil ranks in the moderate range due to delays in 5G deployment. South Africa ranks low, hindered by low connectivity and frequent power outages, while Russia has the lowest 5G penetration among the BRICS countries.

Regarding the ecosystem for innovation, the country's rankings closely mirror those of digital infrastructure. China again leads, dominating in AI patents and benefiting from substantial state-funded R&D. Russia, Brazil and India are medium performers for different reasons. Russia possesses strong research capabilities but the country is hampered by international sanctions. Brazil suffers from low R&D investment and a heavy dependence on foreign technology. India has a favorable environment for innovation, although it faces challenges due to limited funding. South Africa, as the lowest performer, has limited AI patent activity reflectingscarce funding for research and innovation.

In reference to quality of innovation, according to the WIPO's Report on the International Patent System, BRICS countries differ in terms of requirements to patent an innovation.[69] Using the European Patent Organization (EPO) and

Eurasian Patent Organization (EAPO) standards, requiring disclosure "sufficiently clear and complete for it to be carried out by a person skilled in the art," Brazil, India, and South Africa score highest by also demanding the best method of disclosure. China meets only the EPO/EAPO standard without additional requirements, while Russia ranks lowest with a requirement of only disclosing information on the innovation.[70]

Table 3 summarizes these findings, with China emerging as the clear leader, followed by India, Russia, Brazil, and South Africa.

Table 3: Measurement of Economic Variables

Country	**Digital Infrastructure (D.I.)** *(5G internet penetration)*	**Ecosystem for Innovation (E.I.)** *(New patents)*	**Innovation Quality (L.Q.)** (Legal quality requirement for patents)	**Total** *(average)*	**Key Supporting Data**
China	5	5	3	**4.3**	**D.I.**: At least 94 percent of population with 5G access **E.I.**: 1,172 patent per capita; 60 percent global share of AI patents **L.Q.**: clear and complete information to be replicated
Brazil	3	2	4	**3**	**D.I.**: At least 62,7 percent of population with 5G access **E.I.**: 34 patents per capita **L.Q.**: Clear, complete and best method to replicate
India	4	2	4	**3.3**	**D.I.**: At least 82 percent of population with 5G access **E.I.**: 45 patents per capita **L.Q.**: Clear, complete and best method to replicate
Russia	1	3	2	**2**	**D.I.**: No official data available on 5G (but 90 percent of Russians use 4G) **E.I.**: 161 patents per capita **L.Q.**: Only disclosure of information of innovation is required
South Africa	2	1	4	**2.3**	**D.I.**: At least 41,8 percent of population with 5G access **E.I.**: 19 patents per capita **L.Q.**: Clear, complete and best method to replicate

***Digital Infrastructure**: 5 = At least 90 percent of the population have 5G internet access, 4 = Between 90 percent and 70 percent have 5G internet access, 3 = Between 70 percent and 50 percent have 5G internet access, 1 = Less than 30 percent have 5G internet access, 2 = Between 50 percent and 30 percent have 5G internet access, 1 = Less than 30 percent have 5G internet access. Sources: ITU and Izvestia (for Russia).*[71]

***Ecosystem Innovation**: 5 = More than 800 patents per 1M, 4 = Between 800 and 150 patents per 1M, 3 = Between100 and 149 patents per 1M, 2 = Between 30 and 99 patents per 1M, 1 = Less than 30 patents per 1M. Sources: WIPO Country Profile.*[72]
***Innovation Quality**: 5 = Requirements added on top of the ones stated in the previous category, 4 = Clear and complete information plus method of replication, 3 = Clear and complete information on the innovation to be replicated, 2 = Minimal disclose of information on the innovation, 1 = No publicly available criteria. Source: WIPO (2008).*[73]

Governance Variables

Oversight is the core of AI governance. The oversight system is a socio-political construct which is inherently related to formal and informal bureaucratic dynamics in the country. Oversight refers to the creation of an autonomous bureaucracy insulated from social pressures and political capture that can establish and enforce AI compliance requirements. High oversight over AI development indicates the ability, for example, of a country to impose ethical standards. In this article, oversight assesses across countries based on legal AI compliance requirements a country established in its various legislations.

Oversight refers to the creation of an autonomous bureaucracy insulated from social pressures and political capture that can establish and enforce AI compliance requirements

The civilian-military balance is essential to AI governance, as AI's militarization enhances weapon lethality and raises security concerns.[74] In the BRICS context, this balance can be assessed by each country's position on the UN resolution regarding lethal autonomous weapons systems, revealing their approach to regulating the military use of AI. In December 2024, the UN resolution on lethal autonomous weapons passed with support from 166 countries, although China abstained and Russia opposed. The measurement of the civilian-military balance considers two key indicators: a country's military expenditure and its position on the UN resolution.[75] The article presupposes that countries that supported the resolution while maintaining low levels of military spending are more likely to demonstrate a balanced and restrained approach to the military use of AI.

A third variable to measure the AI governance dimension is the trust of society in government AI, which reveals the legitimacy of public institutions in the AI world. Low trust levels are associated in Russia with state control and in South Africa with inequality. Brazil and China are the countries with the highest level of trust, above 60 percent, in government AI among BRICS. Brazil leads in public trust due to healthcare AI successes and NGO monitoring. India's confidence is divided between private and governmental AI, with private AI garnering greater trust. South Africa is at a similar level to India. Russia shows the lowest trust, reflecting societal skepticism of state AI.

Table 4: Measurement of Governance Variables

Country	Oversight (O.) *(AI compliance requirements)*	Civilian-Military Balance (C.M.B.) *(AI Control)*	Public Trust in AI (P.T.) *(Surveys, Civil Society)*	Total *(average)*	Key Supporting Data
China	3	2	5	**3.3**	**O.:** CCP-controlled **C.M.B:** Military-civil fusion; Firms feed military **P.T.:** 67 percent trust in AI
Brazil	4	4	4	**4**	**O.:** 2024 AI Bill (unenforced); Limited public input **C.M.B:** No military AI; Dual-use drones for policing; **P.T.:** 56 percent trust in AI
India	2	3	5	**3.3**	**O.:** No AI laws; Military exempt **C.M.B:** AI border surveillance; DRDO-led R&D **P.T.:** 76 percent trust in AI
Russia	1	1	4	**2**	**O.:** FSB-controlled; No independent oversight **C.M.B:** Military AI dominance (e.g., Lancet drones) **P.T.:** 52 percent trust in AI
South Africa	2	5	4	**3.6**	**O.:** Strong civil society role; Draft AI policy (2024) **C.M.B:** No military AI, Civilian focus **P.T.:** 53 percent trust AI

***Oversight**: 5 = High transparency (highly refined AI compliance requirements), 4 = Moderate-high (refined AI compliance requirements), 3 = Moderate-low (broad and enforceable AI requirements), 2 = Low (non-enforceable AI compliance requirements), 1 = No clear AI compliance requirements. Sources: AI Watch: Global Regulatory Tracker.*[76]
***Civilian-Military Balance**: 5 = A low military spender that supported the UN resolution, 4 = A top-twenty global military spender that supported the UN resolution, 3 = A top-ten global military spender that supported the UN resolution, 2 = A top-five global military spender that abstained in voting the UN resolution, 1 = A top-five global military spender that strongly opposed the UN resolution. Sources: UN and SIPRI.*[77]
***Public Trust in AI**: 5 = High trust above 60 percent. 4 = Moderate trust (40-59 percent). 3 = Moderate-low trust (30-40 percent). 2 = Low trust (10-29 percent). 1 = No data or extreme distrust (<10 percent). Sources: Trust surveys: Brazil, India, China and South Africa ("Trust in AI"); Russia (VCIOM).*[78]

Temporal Variables

Technological speed is a critical factor in assessing a country's potential for AI regulatory readiness. It provides valuable insight into the responsiveness of national policies, particularly in relation to regulatory updates and administrative efficiency. Two indicators are used to measure this dimension: the duration of permits for time-limited AI testing for sandbox experimentation and the average time required for patent approval. These indicators help evaluate, in temporal terms, the institutional readiness to support and adapt to innovation.

South Africa and China emerge as the most responsive countries in terms of technological speed. Both have created favorable environments for the ad-

vancement of sandbox experiments and demonstrate relatively quick policy responses, especially in patent processing. India is not far behind, having significantly reduced the average time required for patent approvals in recent years. Brazil, despite making legislative efforts to regulate AI, continues to lag in establishing a supportive environment for AI development. Russia ranks lowest among the BRICS countries, primarily due to the absence of transparent public procedures related to digital technologies, indicating a limited capacity to support the staged development of AI.

Table 5: Measurement of Temporal Variables

Country	**Tech Speed (T.S.)** *(Speed of Adoption of AI hub)*	**Policy Responsiveness (P.R.)** *(Duration of patent approval)*	**Total** *(average)*	**Key Suporting Data**
China	5	5	**5**	**T.S.**: Leads in AI patents and compute; Rapid industry adoption of tech (e.g., facial recognition) **P.R.**: Backlog doubled to 2.6 million (2021-2022), likely delaying approvals. Average time for patent approval is on average six months
India	4	4	**4**	**T.S.**: Fast startup growth (e.g., AI in agriculture); High research output (STEM focus) **P.R.**: Surge of 149.4 percent in patent grants (2023)
Brazil	3	3	**3**	**T.S.**: Emerging AI hubs (e.g., São Paulo); Moderate compute investment **P.R.**: Reduction of patent backlog by 10.9 percent (2022)
Russia	1	1	**1**	**T.S.**: Absence of AI hub **P.R.**: Lacks public data on backlog reductions
South Africa	4	4	**4**	**T.S.**: Minimal AI R&D; Slow industry adoption **P.R.**: Registration-only system with approx. One year for approval

***Tech Speed**: 5 = Globally dominant AI hub with leading adoption of technology. 4 = Substantial AI hub with high adoption of new tech. 3 = Incipient AI hubs with slow adoption of tech. 2 = Absence of AI hub with slow adoption of tech. 1 = Absence of any tech adoption. Sources: Global Practice Guides of Chambers and Partners (Brazil, China, and India: "Artificial Intelligence 2025" report; South Africa: "Fintech 2022" report).*[79]
***Policy Responsiveness**: 5 = Rapid patent response of 6 months. 4 = Fast patent response of 12 months. 3 = Moderate patent response of 3 to 5 years. 2 = No clear patent response or longer than 5 years. 1 = No clear response or no clear data available. Source: WIPO's Global Innovation Index.*[80]

Regarding patent approval duration, South Africa offers one of the fastest processes, where approval is largely automatic and dependent on the applicant's completion of documentation. China also performs well, with an aver-

Brazil and South Africa focus on equality and fairness of AI access and the effects of deployment, India values the recognition of cultural diversity in the AI models, and China attempts to ensure the safety and reliability of the AI models

age patent approval time of approximately six months, significantly faster than the EU's average of 18 months. India has made notable progress, now averaging between three and five years for patent approvals. This marks a substantial improvement and places India in a moderate performance range. In comparison, Brazil takes slightly over five years on average for patent approvals, reflecting a slower processing bureaucracy. Russia, in contrast, lacks publicly available data on patent timelines, which further underscores its limited institutional transparency and readiness.

Discussions

BRICS Overall Performance and Grouping

The BRICS AI Readiness Index in this article is designed specifically for the five BRICS countries, using relative comparisons among them. Unlike other global indices, *The Oxford Insights Government AI Readiness Index* (GARI), *The Tortoise Media Global AI Index*, and *The Stanford AI Index*, which offer broad overviews, this tailored index provides a more nuanced, context-sensitive assessment aligned with the distinct political, economic, and institutional realities of the BRICS alliance

Among the major global indices, only *GARI 2024* includes all BRICS countries, ranking China (10th), Brazil (24th), Russia (34th), India (45th), and South Africa (77th). These rankings differ from this article's BRICS AI Readiness Index due to varying methodologies and the inclusion of qualitative assessments. As such, the indices should be viewed as complementary rather than conflicting.

GARI 2024 highlights China's AI strength in government capacity, outperforming in the Government Pillar while lagging in digital infrastructure. In 2024, the *GARI Index* evaluated 40 indicators across three core pillars: Government, Technology Sector, and Data and Infrastructure. In contrast, Brazil excels in Data and Infrastructure, followed by Technology, but shows weaker performance in government-related capabilities. These differing profiles reveal distinct national strengths within BRICS.

The largest discrepancies between the indices concern Russia and South Africa. While *GARI 2024* ranks Russia above South Africa, our BRICS AI Readiness

Index reverses this, penalizing Russia for limited data transparency, viewed as a weakness in ethics, governance, and temporal readiness, thus favoring South Africa's more open data practices.

BRICS in AI Ethics: Between Cohesion and Division

The ethics dimension poses a challenge for BRICS given their different focus on the matter. The measurement developed in this article shows similarities between four BRICS members in terms of value alignment and logarithmic accountability, although Brazil ranks slightly higher than China, India, and South Africa due to its stronger framework for value alignment.

Despite these similarities, the countries have different approaches to AI ethics. These are the differences: Brazil and South Africa focus on equality and fairness of AI access and the effects of deployment, India values the recognition of cultural diversity in the AI models, and China attempts to ensure the safety and reliability of the AI models. This means that these countries have different views of how to foster AI transparency and responsibility. However, this does not mean that these countries cannot cooperate on this matter.

Cooperation has been incipient but looks promising, particularly among the democratic BRICS, which have the intention of creating a global governance framework for AI. India is engaged with Brazil, South Africa, and other countries such as Saudi Arabia, South Korea, and the United Arab Emirates to create an "AI for Humanity Agreement."[81]

The Role of Democratic Institutions

Important insights from this article indicate a common tension across BRICS between promoting value alignment in AI and ensuring robust algorithmic accountability, with democratic members tending to emphasize participatory ethics, while authoritarian states prioritize control. This tension seems to be the only effect of democratic institutions on the regulation of AI. This is relevant provided that the ethics dimension is fundamental for the deployment of AI. China, despite not embracing democratic institutions, has a human-centered approach to AI and is willing to build an inclusive AI arena. This is precisely the Chinese uniqueness, as the typology here depicts, which is its capacity to reconcile civilian and military interests.

Another important factor often associated with democratic regimes is the development of trustworthiness within society and in state-society relations, particularly in the context of AI regulation. However, based on the measurement results, trust in governmental use of AI does not appear to be correlated with regime type. A possible explanation for this is that high levels of trust in both AI and government may enhance a government's regulatory legitimacy, suggesting that public trust is more closely linked to perceived regula-

For all BRICS countries and the wider Global South, fostering regional and South-South cooperation, potentially leveraging China's cooperative posture, can support decentralized AI innovation and the development of equitable international regulatory frameworks

tory capacity than to the nature of the political regime itself. Trust is context-dependent, making cross-country comparisons challenging. Furthermore, the use of varying trust indicators across studies complicates the identification of the underlying causes of high or low trust in different countries. What is evident, however, is that China and Russia, despite being non-democratic regimes, display divergent levels of public trust in both their governments and their approach to AI governance.

Misleading Speed-Based Metrics

The measurement of temporal readiness underscores that while rapid responses, such as expedited patent approvals, are important, speed alone does not fully capture the depth of policy responsiveness, especially when transparency and accountability in decision-making are lacking. Moreover, temporal metrics often overlook the quality and effectiveness of decisions. For example, South Africa ranks high in responsiveness to patent approvals, yet its low patent application and approval rate reveals a bureaucratic process that, while fast, reflects a context not conducive to innovation. This example illustrates how speed-based indicators can be misleading when interpreted in isolation from other indicators.

Temporal metrics, nevertheless, remain valuable in assessing a country's capacity to respond to the accelerating demands of a fast-evolving digital environment. They should be interpreted alongside other indicators included in this article's BRICS AI Readiness Index, which provides a more holistic view of institutional performance.

Conclusion

This analysis has sought to evaluate the AI regulatory readiness of Brazil, Russia, India, China, and South Africa, exploring their capacities to manage AI's consequences and their potential roles in shaping global governance.

The study highlights varied levels of AI readiness among BRICS countries. China leads with a "Capable Hybrid Oversight" model, combining civilian and military AI use under strong state control. Brazil, India, and South Africa follow a "Democratic Governance" model with mixed strengths: Brazil has a

balanced performance across different dimensions, India excels economically and temporally, and South Africa shows strong governance. Russia, under "Authoritarian Control," focuses on military AI but lags behind overall. No BRICS country fits the "Laissez-Faire Democratic Governance" model.

Addressing the regulatory capacity, this research suggests that while BRICS countries are actively developing frameworks, their ability to manage AI's societal impact varies. To navigate this complex future, tailored policy recommendations are crucial:

- China should implement stricter dual-use export controls to mitigate global AI arms races and continue to refine its ethical guidelines to better incorporate broad human well-being.
- Russia faces the need for increased international scrutiny regarding AI warfare risks and must work towards greater transparency and the establishment of independent oversight mechanisms for AI development and deployment.
- India needs to formalize AI legislation, clarify vague terms such as "harmful AI," and enhance mechanisms for algorithmic accountability to ensure robust democratic oversight amid growing dual-use AI technologies.
- Brazil should extend AI regulation to the private sector, secure sufficient funding for the National Authority for Data Protection (ANPD) to enable effective oversight and tackle long-term challenges in AI governance.
- South Africa has the potential to become a leader in ethical AI governance in the Global South with the democratic approval of its IA framework. Important steps include establishing a centralized regulatory authority to overcome fragmentation and addressing constraints on human capital and financial resources.

For all BRICS countries and the wider Global South, fostering regional and South-South cooperation, potentially leveraging China's cooperative posture, can support decentralized AI innovation and the development of equitable international regulatory frameworks. Enacting flexible, innovation-friendly regulations, establishing dedicated AI governance agencies, and developing policies to address AI's economic impacts, such as the productivity paradox and workforce displacement, are vital measures.

This article acknowledges certain limitations, including its reliance on qualitative assessments for some variables and the challenge of fully capturing the real-world application of rapidly evolving legal frameworks from textual analysis of legislations and strategic plans. The dynamic nature of AI itself means that the findings represent a snapshot of a constantly changing field.

Another limitation concerns data used for China and Russia, which might reflect a "visibility bias." Evaluating countries that produce untransparent

published data carries an inherent risk of "visibility bias," which the article attempted to overcome through data triangulation. For example, China's rapid patent approvals (temporal dimension) contrast with its lower patent quality standards (economic dimension) compared to Brazil, India, and South Africa, highlighting discrepancies between speed and legal rigor.

Future research should focus on longitudinal analyses to track the evolution of AI readiness in BRICS countries. Deeper investigations into the practical implementation and effectiveness of national AI strategies are needed, moving beyond legislative texts. Developing more nuanced indicators, especially for the temporal dimension (such as AI adoption lag and policy update frequency) and the ethical dimension, will provide a more comprehensive understanding of the progress of AI regulation. Comparative studies with other Global South countries could also yield valuable insights into shared challenges and successful AI governance models. To provide a more comprehensive perspective that official data does not convey in opaque regimes (e.g., China, Russia), it may be necessary to turn to alternative methods such as interviews with officials, technologists, and civil society actors. These interviews would offer a more substantive comprehension that official data cannot encapsulate.

While BRICS countries are at different stages of AI regulatory readiness, their collective actions and individual commitments to responsible AI governance will be pivotal in shaping a future in which AI's benefits are maximized and its risks are effectively managed for a more equitable global order.

Endnotes

1. "Getting The UK's Legislative Strategy for AI Right," *Tony Blair Institute for Global Change*, (September 2024), retrieved from https://institute.global/insights/tech-and-digitalisation/getting-the-uks-legislative-strategy-for-ai-right; "AI 2027: Superhuman Systems and a Global Security Crisis?" *AI Futures Project*, (April 4, 2025), retrieved from https://ai-2027.com/.

2. "Getting The UK's Legislative Strategy for AI Right."

3. Sharma Ams, "Blurred Lines: The Convergence of Military and Civilian Uses of AI and Data Use and Its Impact on Liberal Democracy," *International Politics*, Vol. 60, (2023), pp. 879-896.

4. "Freedom on the Net 2023," *Freedom House*, (2023), retrieved from https://freedomhouse.org/sites/default/files/2024-10/FOTN2023Final24.pdf.

5. "Democratizing AI: Principles for Meaningful Public Participation," *Data and Society*, (2023), retrieved from https://datasociety.net/wp-content/uploads/2023/09/DS_Democratizing-AI-Public-Participation-Brief_9.2023.pdf.

6. Paul Timmers, "Ethics of AI and Cybersecurity When Sovereignty Is at Stake," *Minds and Machines*, Vol. 29, (2019), pp. 635-645; Marvin Hanisch, Curtis M. Goldsby, Nicolai E. Fabian, and Jana Oehmichen, "Digital Governance: A Conceptual Framework and Research Agenda," *Journal of Business Research*, Vol. 162, (2023).

7. Eva Erman and Markus Furendal, "Artificial Intelligence and the Political Legitimacy of Global Governance," *Political Studies*, Vol. 72, No. 2 (2022), pp. 421-441.

8. Adib Bin Rashid, Ashfakul Karim Kausik, Ahamed al Hassan Sunny, and Mehedy Hassan Bappy, "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges," *International Journal of Intelligent Systems*, Vol. 2023, (2023), pp. 1-31.

9. Dominique Verdejo and Eunika Mercier Laurent, "How Can LLM Improve Efficiency of C4ISR?" in Dominique Verdejo and Eunika Mercier Laurent (eds.), *Artificial Intelligence for Global Security: AI4GS 2024*, (Cham: Springer, 2025), pp. 1-17.

10. Johannes Thumfart, "The Democratic Offset: Contestation, Deliberation, and Participation Regarding Military Applications of AI," *AI Ethics*, Vol. 4, (2024), pp. 511-526.

11. "Brazil: Bill 21/2020 Approved by House of Representatives," *Digital Policy Alert*, retrieved July 9, 2025, from https://digitalpolicyalert.org/event/931-bill-212020-approved-by-house-of-representatives.

12. "Regulatory Framework for Artificial Intelligence Passes in Brazil's Senate," *Advocacia Mattos Filho*, (December 11, 2024), retrieved July 9, 2025, from https://www.mattosfilho.com.br/en/unico/framework-artificial-intelligence-senate/.

13. "Getting the UK's Legislative Strategy for AI Right."

14. "Plano Brasileiro de Inteligência Artificial (PBIA) 2024-2028," *Ministry of Science, Technology and Innovation*, (August 7, 2024), retrieved from https://www.gov.br/lncc/pt-br/assuntos/noticias/ultimas-noticias-1/plano-brasileiro-de-inteligencia-artificial-pbia-2024-2028.

15. "How the Digital India Act Will Shape the Future Of The Country's Cyber Landscape," *The Hindu*, (October 9, 2023), retrieved from https://www.thehindu.com/sci-tech/technology/how-the-digital-india-act-will-shape-the-future-of-the-countrys-cyber-landscape/article67397155.ece.

16. "South Africa National AI Policy Framework," Department of Communications and Digital Technologies, (September 3, 2011), retrieved from https://www.dcdt.gov.za/sa-national-ai-policy-framework.html.

17. Republic of South Africa, "Protection of Personal Information Act (No. 4 of 2013)," *Government Gazette*, Vol. 581, No. 37067 (2013), retrieved July 10, 2025, from https://www.gov.za/documents/protection-personal-information-act.

18. Republic of South Africa, "Cybercrimes Act 2020," *Government Gazette*, Vol. 672, No. 44651 (June 1, 2021), retrieved July 10, 2025, from https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf.

19. ST Mota Makore, "Regulating Artificial Intelligence to Advance Financial Inclusion in South Africa," *Potchefstroom Electronic Law Journal (PELJ)* Vol. 27, No. 1 (2024), pp. 1-35.

20. "Decree of the President of the Russian Federation on the Development of Artificial Intelligence in the Russian Federation," *Center for Security and Emerging Technology,* (October 28, 2019), retrieved July 9, 2025, from https://cset.georgetown.edu/wp-content/uploads/Decree-of-the-President-of-the-Russian-Federation-on-the-Development-of-Artificial-Intelligence-in-the-Russian-Federation-.pdf

21. "Russia Adopts Law on Regulatory Sandboxes," *Debevoise Update*, *Debevoise and Plimpton*, (September 18, 2020), retrieved from https://www.debevoise.com/-/media/files/insights/publications/2020/09/20200918-russian-law-on-regulatory-sandboxes-eng.pdf?rev=5fb274e559134bfc98f925e9b8ed9708&hash=10DF3C1649E0F0CA4D86609AAB95E232.

22. Samuel Bendett, "The Role of AI in Russia's Confrontation with the West," *Center for a New American Security,* (April 1, 2024), pp. 3-8.

23. Justin Sherman, "Russia's Internet Censor Is Also a Surveillance Machine," *Council of Foreign Relations*, (September 28, 2022), retrieved May 25, 2025, from https://www.cfr.org/blog/russias-internet-censor-also-surveillance-machine.

24. Andrea Gilli and Mauro Gilli, "Appraising the State of Play of C4ISR Infrastructure within NATO Gaps, Deficiencies and Steps Forward," *The Hague Center of Strategic Studies*, (2025), retrieved May 16, 2025, from https://hcss.nl/report/appraising-the-state-of-play-of-c4isr-infrastructure-within-nato-gaps-deficiencies-and-steps-forward/.

25. Katarzyna Zysk, "Struggling, not Crumbling: Russian Defence AI in a Time of War," *RUSI*, (November 20, 2023), retrieved June 23, 2025, from https://www.rusi.org/explore-our-research/publications/commentary/struggling-not-crumbling-russian-defence-ai-time-war.

26. "Data Security Law of the People's Republic of China," *The National People's Congress of the People's Republic of China,* retrieved July 9, 2025, from http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html.

27. "Personal Information Protection Law of the People's Republic of China," *The National People's Congress of the People's Republic of China,* retrieved July 9, 2025, from http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

28. "China: Generative AI Measures Finalized, Library of Congress," *Library of Congress,* retrieved July 9, 2025, from https://www.loc.gov/item/global-legal-monitor/2023-07-18/china-generative-ai-measures-finalized/.

29. "AI Safety Governance Framework," *National Technical Committee 260 on Cybersecurity of SAC 2024,* (September, 2024), retrieved from https://www.tc260.org.cn/upload/2024-09-09/1725849192841090989.pdf

30. Genia Kostka, "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval," *New Media and Society* Vol. 21, No. 7 (2019), pp. 1565-1593.

31. Jing Cheng, "Contextualizing China's AI Governance," *Global Policy Journal*, (June 1, 2023), retrieved May 25, 2025, from https://www.globalpolicyjournal.com/blog/01/06/2023/contextualizing-chinas-ai-governance.

32. James Johnson, *The US-China Military and Defense Relationship during the Obama Presidency*, (Cham: Palgrave Macmillan, 2018), pp. 65-94.

33. Guangyu Qiao-Franco and Ingvild Bode, "Weaponised Artificial Intelligence and Chinese Practices of Human-Machine Interaction," *The Chinese Journal of International Politics*, Vol. 16, No. 1 (2023), pp. 106-128.

34. Daniel Susser, "Decision Time: Normative Dimensions of Algorithmic Speed," *FAccT*, (June 20, 2022), retrieved July 7, 2025, from https://doi.org/10.1145/3531146.3533198.

35. Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence,* (New Haven: Yale University Press, 2021), p. 137.

36. Thilo Hagendorff, "The Ethics of AI Ethics: An Evaluation of Guidelines," *Minds and Machines*, Vol. 30, (2020), pp. 99-120.

37. Abhishek Sharma, "Temporal Reasoning in AI Systems," *arXiv preprint,* (2025), retrieved from https://doi.org/10.48550/arXiv.2502.00020.

38. Ethan Fast and Eric Horvitz, "Long-Term Trends in the Public Perception of Artificial Intelligence," *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 31, No. 1 (2017), retrieved from https://doi.org/10.1609/aaai.v31i1.10635.

39. Zhifa Ke, Zaiwen Wen, and Junyu Zhang, "An Improved Finite-time Analysis of Temporal Difference Learning with Deep Neural Networks," *ICML'24: Proceedings of the 41st International Conference on Machine Learning*, No. 943, (2024), pp. 2340-2342.

40. Lucia M. Rafanelli, "Justice, Injustice, and Artificial Intelligence: Lessons from Political Theory and Philosophy," *Big Data and Society*, Vol. 9, No. 1 (2022).

41. Andreas Matthias, "The Responsibility Gap: Ascribing Responsibility for The Actions of Learning Automata," *Ethics and Information Technology*, Vol. 6, No. 3 (2004), pp. 175-183.

42. Lazaros Jason Anastasopoulos and Andrew Brian Whitford, "Machine Learning for Public Administration Research, with Application to Organizational Reputation," *Journal of Public Administration Research and Theory*, Vol. 29, No. 3 (2019), pp. 491-510.

43. Iason Gabriel, "Artificial Intelligence, Values, and Alignment," *Minds and Machines*, Vol. 30, (2020), pp. 411-437.

44. David J. Gunkel, *The Machine Question: Critical Perspectives on AI, Robots, and Ethics,* (Cambridge: The MIT Press, 2012).

45. Han Yu, Zhiqi Shen, Chunyan Miao, Cyril Leung, Victor R. Lesser, and Qiang Yang, "Building Ethics into Artificial Intelligence," *arXiv preprint,* (2018), retrieved from https://arxiv.org/abs/1812.02953.

46. Winnie Ma and Vincent Valton, "Toward and Ethics of AI Belief," *Philosophy and Technology*, Vol. 37, No. 76 (2024).

47. Vicky Charisi, Louise Dennis, Michael Fisher, Robert Lieck, Andreas Matthias, Marija Slavkovik, Janina Sombetzki, Alan F. T. Winfield, and Roman Yampolskiy, "Towards Moral Autonomous Systems," *arXiv preprint,* (2017), retrieved from https://arxiv.org/abs/1703.04741.

48. Joanna J. Bryson, "Patiency Is Not a Virtue: The Design of Intelligent Systems and Systems of Ethics," *Ethics and Information Technology*, Vol. 20, (2018), pp. 15-26.

49. David Adam, "Lethal AI Weapons Are Here: How Can We Control Them?" *Nature*, No. 629 (April 23, 2024), retrieved June 23, 2025, from https://doi.org/10.1038/d41586-024-01029-0, pp. 521-523.

50. Anna Jobin, Marcello Ienca, and Effy Vayena, "Artificial Intelligence: The Global Landscape of Ethics Guidelines," *Nature Machine Intelligence*, Vol. 1, No. 9 (2019), pp. 389-399.

51. Dan Hendrycks, Collin Burns, Steven Basart, Andrew Critch, Jerry Li, Dawn Song, and Jacob Steinhardt, "Aligning AI with Shared Human Values," *arXiv preprint,* (2020), retrieved from https://arxiv.org/abs/2008.02275.

52. Jonas Tallberg, Eva Erman, Markus Furendal, Johannes Geith, Mark Klamberg, and Magnus Lundgren, "The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research," *International Studies Review*, Vol. 25, No. 3 (2023), p. 40.

53. Marvin Hanisch, Curtis M. Goldsby, Nicolai E. Fabian, and Jana Oehmichen, "Digital Governance: A Conceptual Framework and Research Agenda," *Journal of Business Research*, Vol. 162, (2023), p. 113777.

54. Peter Cihon, Matthijs Maas, and Luke Kemp, "Should Artificial Intelligence Governance Be Centralised? Design Lessons from History," *arXiv preprint,* (2020), retrieved May 25, 2025, from https://arxiv.org/abs/2001.03573.

55. Sharma Ams "Blurred Lines: The Convergence of Military and Civilian Uses of AI and Data Use and Its Impact on Liberal Democracy," *International Politics*, Vol. 60, (2023), pp. 879-896.

56. Sophie-Charlotte Fischer and Andreas Wenger, "Artificial Intelligence, Forward-Looking Governance and the Future of Security," *Swiss Political Science Review*, Vol. 27, No. 1 (2021), pp. 170-179.

57. Johannes Thumfart, "The Democratic Offset: Contestation, Deliberation, and Participation Regarding Military Applications of AI," *AI Ethics*, Vol. 4, (2024), pp. 511-526.

58. Lucia M. Rafanelli," Justice, Injustice, and Artificial Intelligence: Lessons from Political Theory and Philosophy," *Big Data and Society*, Vol. 9, No. 1 (2022); Vincent J. Straub, Deborah Morgan, Jonathan Bright, and Helen Margetts, "Artificial Intelligence in Government: Concepts, Standards, and a Unified Framework," *Government Information Quarterly*, Vol. 40, No. 4 (2023), p. 101881.

59. "2023 Edelman Trust Barometer: The Trust Gap in AI," *Edelman,* (2023), retrieved from https://www.edelman.com/trust/2023/trust-barometer/ai-and-trust.

60. Erik Brynjolfsson and Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, (New York: W. W. Norton and Company, 2014).

61. Anton Korinek and Joseph E. Stiglitz, "Artificial Intelligence, Globalization, and Strategies for Economic Development," *National Bureau of Economic Research*, (January 2021), retrieved from https://www.nber.org/papers/w28453.

62. Mariarosaria Comunale and Andrea Manera, "The Economic Impacts and the Regulation of AI: A Review of the Academic Literature and Policy Actions," *International Monetary Fund*, (March 22, 2024), retrieved from https://www.imf.org/en/Publications/WP/Issues/2024/03/22/The-Economic-Impacts-and-the-Regulation-of-AI-A-Review-of-the-Academic-Literature-and-546645.

63. Henning Vöpel, "The AI Revolution: A New Paradigm of Economic Order," *The Economists' Voice*, Vol. 2, No. 2 (2024), pp. 345-355.

64. Mauro Cazzaniga, Florence Jaumotte, Longji Li, Giovanni Melina, Augustus J. Panton, Carlo Pizzinelli, Emma J. Rockall, and Marina Mendes Tavares, "Gen-AI: Artificial Intelligence and the Future of Work," *International Monetary Fund*, (January 14, 2024), retrieved from https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2024/01/14/Gen-AI-Artificial-Intelligence-and-the-Future-of-Work-542379.

65. "OECD AI Principles," *Organisation for Economic Co-operation and Development*, (2023), retrieved May 21, 2025, from https://www.oecd.org/going-digital/ai/principles.

66. "AI Watch: Global Regulatory Tracker," *White and Case*, retrieved May 16, 2025, from https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker.

67. "AI Watch: Global Regulatory Tracker," *White and Case*.

68. Kyle Higham, Gaétan de Rassenfosse, and Adam B. Jaffe, "Patent Quality: Towards a Systematic Framework for Analysis and Measurement," *Research Policy*, Vol. 50, No. 4 (2021), p. 104215.

69. "Report on the International Patent System," *World Intellectual Property Organization (WIPO)*, (2008), retrieved from https://www.wipo.int/edocs/mdocs/scp/en/scp_12/scp_12_3.pdf.

70. "Report on the International Patent System: Annex II, Sufficiency of Disclosure," *World Intellectual Property Organization (WIPO)*, (2008), retrieved from https://www.wipo.int/export/sites/www/scp/en/national_laws/disclosure.pdf.

71. "ITU Data Hub, Connectivity," *ITU*, (2023), retrieved June 21, 2025, from https://datahub.itu.int/data/; "Grigorenko Announced the Access of more than 90 percent of the Russian Population to 4G Communications," *Izvestia*, (June 6, 2025), retrieved June 25, 2025, from https://en.iz.ru/en/1899838/2025-06-06/grigorenko-announced-access-more-90-russian-population-4g-communications.

72. "Report on the International Patent System: Annex II, Sufficiency of Disclosure."

73. "Report on the International Patent System: Annex II, Novelty," *World Intellectual Property Organization (WIPO)*, (2008), retrieved from https://www.wipo.int/export/sites/www/scp/en/national_laws/novelty.pdf.

74. Denise Garcia, *The AI Military Race: Common Good Governance in the Age of Artificial Intelligence,* (Oxford: Oxford University Press, 2023), pp. 10-11.

75. "Lethal Autonomous Weapons Systems: Resolution," *United Nations' General Assembly*, (December 2, 2024), retrieved June 22, 2025, from https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2024.

76. "AI Watch: Global Regulatory Tracker."

77. "Lethal Autonomous Weapons Systems: Resolution," *United Nations*, retrieved from https://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2024; "Trends in World Military Expenditure, 2022," *SIPRI,* (April 2023), retrieved June 23, 2025, from https://www.sipri.org/sites/default/files/2023-04/2304_fs_milex_2022.pdf.

78. "Trust in Artificial Intelligence: A Global Study," *The University of Queensland and KPMG Australia*, (2023), retrieved May 16, 2025, from https://ai.uq.edu.au/project/trust-artificial-intelligence-global-study; "Trust in AI," *VCIOM – Russia Public Opinion Research Center*, (December 24, 2024), retrieved from https://wciom.com/press-release/trust-in-ai.

79. "Artificial Intelligence 2025," *Chambers and Partners*, (2025), retrieved May 22, 2025, from https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2025; "Fintech 2022: South Africa," *Chambers and Partners*, (2022), retrieved May 22, 2025, from https://chambers.com/downloads/gpg/656/034_south_africa.pdf.

80. "Global Innovation Index 2024: Unlocking the Promise of Social Entrepreneurship," *WIPO*, (2024), retrieved May 22, 2025, from https://www.wipo.int/web-publications/global-innovation-index-2024/assets/67729/2000%20Global%20Innovation%20Index%202024_WEB3lite.pdf.

81. Sundeep Waslekar, "India's AI Gambit: Exploring our Strategic Options," *NatSrat: Center for Research on Security and Strategic Issues*, (May 20, 2025), retrieved May 25, 2025, from https://www.natstrat.org/articledetail/publications/india-s-ai-gambit-exploring-our-strategic-options-199.html#.