OPINION

AI and the Fragmentation of Legal Sovereignty: A Comparative Analysis in BRICS Nations

Saslina Kamaruddin,
Tashkent State University of Law (Tashkent, Uzbekistan)
https://orcid.org/0000-0002-7356-3846

Muhammad Izwan Ikhsan,
MARA University of Technology (Kota Kinabalu, Malaysia)
https://orcid.org/0000-0003-2635-0909

Navtika Singh Nautiyal,
National Forensic Sciences University (Gandhinagar, India)
https://orcid.org/0009-0007-7004-178X

https://doi.org/10.21684/2412-2343-2026-13-2-184-207

Received: January 20, 2026
Reviewed: April 4, 2026
Accepted: May 6, 2026

Abstract. In the 21st century, state sovereignty is undergoing a profound transformation, largely driven by advances in artificial intelligence (AI) and the changing landscape of jurisprudential autonomy and structural power. This article explores how AI is challenging traditional notions of sovereignty and influencing states in the interaction with each other and with emerging technologies. The study discusses the ethical and legal dilemmas raised by artificial intelligence, focusing on decision-making procedures, surveillance tools, and regulations on data use. Additionally, it discusses the geopolitical ramifications of AI development, emphasizing the possibility of shifts in power and global competitiveness. Drawing from case studies and scholarly insights, the article suggests that AI's evolution necessitates reimagining sovereignty, moving towards a more fluid and networked

governance model. It underscores the need for global cooperation and ethical frameworks to ensure AI's responsible development and deployment while safeguarding individual rights and democratic principles.

Keywords: state sovereignty; artificial intelligence; technology; law; BRICS; Brazil; Russia; India; China.

To cite: Kamaruddin, S., Ikhsan, M. I., & Nautiyal, N. S. (2026). AI and the fragmentation of legal sovereignty: A comparative analysis in BRICS nations. *BRICS Law Journal*, *13*(2), 184–207.

Table of Contents

Introduction

In an era of unprecedented technological advancements, artificial intelligence (AI) has emerged as a transformative force, reshaping societies, economies, and even the fabric of human consciousness. The implications of AI extend beyond mere automation and data analysis, touching upon fundamental concepts such as sovereignty and the evolving nature of human thought and awareness. The rise of AI challenges traditional notions of sovereignty in multiple dimensions. On the one

hand, it empowers nations with enhanced governance, economic management, and defense capabilities. AI-driven systems can predict economic trends, optimize resource allocation, and enhance national security through sophisticated surveillance and defense mechanisms. However, this technological advancement also poses significant risks. The centralization of AI expertise and resources in a few dominant countries or corporations can undermine the sovereignty of smaller nations, creating dependencies and exacerbating geopolitical imbalances. Furthermore, the global nature of AI technology necessitates international cooperation and regulation, challenging the traditional sovereignty paradigm that emphasizes autonomous, nation-centric governance.

The convergence of AI with sovereignty and consciousness highlights a complex interplay of empowerment, dependence, innovation, and ethical dilemmas. Nations are grappling with the challenge of harnessing AI's potential while safeguarding their sovereignty and ethical integrity. Simultaneously, individuals and societies must navigate the profound shifts in consciousness prompted by AI's pervasive influence. The transformation brought about by AI is not merely technological; it is deeply philosophical and existential, prompting questions about the nature of human experience and the future of civilization.

The exploration of AI, sovereignty, and changing consciousness offers a lens to examine the multifaceted impact of AI on the world. It underscores the need for a nuanced understanding of how technology shapes external realities and internal landscapes, ultimately influencing human evolution. As we embark on this new era, the dialogue around AI must expand these broader implications, fostering a holistic approach to navigating the challenges and opportunities that lie ahead.

1. Methodology

To investigate the profound transformation of state sovereignty driven by artificial intelligence (AI), this study adopts a qualitative, multidisciplinary methodology situated at the intersection of international relations theory and comparative legal analysis. By examining the case studies of national AI strategies, surveillance tools, and regulations on data use, the research assesses shifts in structural power and global competitiveness to propose a fluid, networked governance model. This macro-level, state-centric approach contrasts sharply with foundational, micro-level analyses of AI's legal status, such as those grounded in quantum cognitive science.

While the present study focuses on the systemic redistribution of geopolitical power, contemporary research investigates whether AI entities inherently possess the capability for legal personhood and capacity. Utilizing quantum theory, researchers mathematically differentiate classical AI, which relies on deterministic algorithms to resolve merely subjective uncertainty, from natural intelligence, resolving objective quantum uncertainty to generate genuine free will, affective meaning, and novelty.

Because classical AI is limited to algorithmic computation, it fundamentally lacks true autonomy, legal subjectivity, and genuine decision-making capabilities. Consequently, such foundational studies conclude that classical AI cannot hold legal capacity under civil or common law requiring that all legal and moral responsibility remains strictly with human creators and users. Thus, while this paper explores how AI advancements challenge global governance and necessitate global cooperation, it must recognize that the underlying physical and ontological limits of classical AI preclude the technology itself from attaining independent legal agency.

2. Conceptual Framework

2.1. Conceptualizing Sovereignty

Conceptualizing sovereignty is a multifaceted task that involves exploring its historical, political, legal, and philosophical dimensions. At its core, sovereignty refers to the supreme authority of a state to govern itself within its borders without interference from external actors. Nonetheless, when issues such as globalization, human rights, and international law challenge on long-held notions in today's interconnected world, discussions on sovereignty sometimes struggle with its complexity. Scholars debate whether sovereignty is immutable or becoming a more complex idea that takes accountability to the international community and responsibility into account. To fully comprehend sovereignty and its relevance in forming the contemporary international order, exploring its diverse interpretations in various situations and academic fields is necessary. Bodin and Hobbes suggest the traditional meaning of sovereignty in terms of "Domestic Sovereignty," which expresses the authority or supremacy over a particular state or boundary, which means the right to govern within a state.[1] The more advanced meaning dealt with through globalization, we consider "interdependence sovereignty."[2] Daniel Philpott visualized sovereignty in terms of authority, and it becomes legitimate when it is rooted in law and divine command or when it gains the assent of the people who consent to exercise it over themselves to protect their interests. Even absolutists like Hobbes and Bodin trace the root of sovereignty to protecting some people's rights. This understanding of sovereignty, based on the protection of people's interests, created space for the development of sovereignty in the modern sense.

Sovereignty is one of the constituent ideas of the post-medieval world; it conveys a distinctive configuration of politics and law that sets the modern era apart from previous eras.[3] According to Philpott, sovereignty must have four elements: 1) power;

---

[1] Bodin, J. (1992). *On sovereignty: Four chapters from the six books of the commonwealth*. Cambridge University Press; Hobbes, T. (1968). *Leviathan*. Penguin Books.

[2] Philpott, D. (2001). Usurping the sovereignty of sovereignty? *World Politics, 53*(2), 297–324.

[3] Grittersová, J. (1999). The evolution of the concept and the role of sovereignty. *Medzinárodné otázky*, 105–117.

2) legitimacy drawn from "any mutually recognized source of legitimacy, such as God, a constitution, or inherited law"; 3) supremacy; and 4) control over a territory. International relations are still framed by the spatial aspect of sovereignty today.[4] In particular, the idea of state sovereignty, or Westphalian sovereignty, refers to the supreme authority of a ruling body (whether it is a monarch or a legally elected parliament) over the territory and internal affairs of the state, free from intervention by outside forces.[5] George Sorenson puts the point very well: the importance of the sovereignty doctrine can hardly be overrated. It was a formidable tool for lawyers and politicians and a decisive factor in modern Europe. Sovereignty is a foundational idea of politics that determines the domain of authority in the marked border of any country.[6] We can trace the origin and history of sovereignty which consists of an intense relation with the nature and evolution of the state, especially to the development of "centralized authority in early modern Europe, which also shaped the relationship between the state and civil society and between "political community."[7] The originality of modern sovereignty is often obscured in comparison with "analogous mentally different conceptions" in the Greek city-states, Egyptian and Roman empires, and the kingdoms and principalities of Europe.[8] The decentralized political arrangements of the feudal system created space for the modern notion of sovereignty that entitled to the Westphalian political system, while in terms of meaning, it was defined as "Supreme Normative Power with a domain."[9] From the Middle Ages, when there was a clash for establishing authority, almost none of it became an authority; the emergence of sovereignty was shaped by the religious conflicts associated with the Reformation and the subsequent establishment of the Westphalian system.[10] For Bodin and Hobbes, the discourse of modern sovereignty suggests that a legitimate sovereign is not above human law but a source of it. Since the 18th century, this approach has changed. With Western states' constitutional advancement and virtual presence everywhere, human lawmakers or lawgivers do not entail legitimate sovereign authority. Instead, constitutions and international legal agreements define the scope of all rulers' and citizens' legitimate authority.[11]

---

4 Philpott, D. (2016). Sovereignty. In E. N. Zalta (Ed.). *The Stanford encyclopedia of philosophy*. Metaphysics Research Lab, Stanford University.

5 Couture, S., & Toupin, S. (2017). *What does the concept of sovereignty mean in digital, network and technological sovereignty?* GigaNet: Global Internet Governance Academic Network, Annual Symposium. https://doi.org/10.2139/ssrn.3107272

6 Sørensen, G. (1999). Sovereignty: Change and continuity in a fundamental institution. *Political Studies, 47*(3), 590–604.

7 Sørensen, 1999.

8 Grittersová, 1999.

9 Nunez, J. E. (2014). *Shared sovereignty in a two State context: A problem of distributive justice*. The University of Manchester (United Kingdom).

10 Philpott, 2016.

11 Philpott, D. (1999). Westphalia, authority, and international society. *Political Studies, 47*(3), 566–589.

One of Philpott's key arguments is that sovereignty is not just about power or control but also about responsibility. He suggests that sovereign states must protect their citizens' human rights and dignity and that this duty extends to all individuals, regardless of their religious or cultural background. In his view, sovereignty is not just a right granted to states but also a responsibility they must fulfil.[12] According to Henkin, the concept of state sovereignty and its application to international law are, at best, undeserving and, at worst, "destructive of human values." Henkin makes it quite evident what belongs in the second category, even though it is unclear what qualifies as unworthy. When the concept of state sovereignty is employed to absolve states and their leaders of responsibility under international law for violating human rights or sabotaging international collaboration, it undermines human values.[13]

2.2. AI's Dual Impact: Challenges to and Reinforcement of Sovereignty

2.2.1. The Impact of AI on State Sovereignty

Artificial intelligence is revolutionizing various aspects of governance, economy, and society, challenging the conventional boundaries of state sovereignty. One important area of impact is information warfare and cybersecurity, where non-state actors can influence or disrupt sovereign state affairs without directly intervening in their territory, thanks to AI-powered tools. Concerns are also raised regarding states' capacity to retain exclusive control over the use of force within their borders due to the spread of autonomous weapons systems. The advent of AI has prompted a reassessment of sovereignty. Some academics contend that AI challenges state sovereignty by empowering non-state entities to wield influence and power in unprecedented ways.[14] For instance, AI can facilitate cyberattacks capable of profoundly affecting a nation's security and stability. The deployment of AI in developing and operating autonomous weapons systems has become a contentious issue, raising significant ethical, legal, and security concerns.[15] Others argue that AI technologies simultaneously strengthen state sovereignty by enhancing governments' ability to monitor and control their populations. This perspective emphasizes the role of AI in bolstering state power through advanced surveillance systems, data analytics, and predictive policing.[16]

The use of AI in border control and immigration has enabled states to manage their borders and regulate the movement of people and goods more effectively.

---

[12] Philpott, 1999.

[13] Henkin, L. (1995). Human rights and state sovereignty. *Georgia Journal of International and Comparative Law, 25*, 31–46.

[14] Timmers, P. (2019). Ethics of AI and cybersecurity when sovereignty is at stake. *Minds and Machines, 29*(4), 635–645.

[15] Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law, 25*, 273–291.

[16] Usman, H., Nawaz, B., & Nasser, S. (2023). The future of state sovereignty in the age of artificial intelligence. *Journal of Law & Social Studies, 5*(2), 142–152.

While state sovereignty remains a key pillar of the international system, it has been increasingly challenged by globalization and new technologies like AI. AI can either weaken or reinforce state sovereignty, making its impact a continuously evolving subject of study.

2.2.2. AI and the Global Economy

In the economic realm, AI-driven automation and digital platforms are reshaping global supply chains and labor markets, undermining the capacity of states to regulate economic activities within their jurisdictions. The rise of digital currencies and decentralized finance further complicates traditional notions of monetary sovereignty, as states grapple with the challenges posed by borderless financial systems. The traditional understanding of sovereignty, recognized as one of the essential components of the Westphalian state system, the contemporary political system, and global power relations, cannot adequately address what sovereignty is meant to achieve. Confusion is nevertheless caused by its shifting nature. Nowhere in history has modern sovereignty evolved during a period when the territory was the land and sea, the population was primarily composed of settled individuals, and the activities conducted by the people within these territories were visible and tangible.[17]

Government leaders feel that national sovereignty is under threat. Timmers explains the reason as a confluence of pervasive, transformative, and disruptive digital technologies leading to the explosive growth of cyber incidents, rising international tensions between the US and EU on one side, China and Russia on the other, and transatlantic tensions.[18] There is no doubt that these threats put sovereignty at stake. Kello argues that "cyber" creates a "sovereignty gap." Both state and non-state actors are exploiting cyber capabilities.[19] Kello observes a combination of persistent disruption ("unpeace"), rogue state actors that misuse cyber technologies, and cyber-enabled exercise of influence by non-state actors, from state proxies to terrorists to global platforms, that systematically alter the balance of power in the traditional state-based (Westphalian) system of international relations. A critical assessment of the decline of the traditional vision of sovereignty and its deficiencies allows to identify emerging concepts such as data sovereignty, digital sovereignty, and technological sovereignty.

This newly emerging dimension of sovereignty is creating a new space of sovereign authority that shifts power from traditional sovereign authorities, such as the state or government, to technocrats, and the final implication of this new

---

[17] Aydın, A., & Bensghir, T. K. (2019). Digital data sovereignty: Towards a conceptual framework. In *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, 1–6.

[18] Timmers, 2019.

[19] Kello, L. (2023) The state in the digital era. In *Digital international relations* (pp. 51–72). Taylor & Francis.

dimension compromises the autonomy of sovereign states. Yuval Noah Harari warned that the world is becoming too dependent on data-driven technologies. The consequences take us toward data colonialism, which can consolidate the power of monopolistic corporations and tyrannical governments.[20] While addressing the National Association of Software and Services Companies (NASSCOM) Leadership Summit in 2022, he predicted the world of data colonialism as one of the biggest dangers to the human future. He mentioned that a larger amount of data in the form of artificial intelligence and machine learning poses two big challenges to governments and the public alike.[21] Harari points out that not even the dictators and tyrants of the past could do this because they did not have the required technologies, so the only way out is to prevent such regimes and situations. He also emphasized that in the 21st century, one country does not need to send in its soldiers to conquer another nation; all it needs to do is to obtain data on its leaders and people. "Imagine a situation wherein China or the US has the entire personal records of a country's politicians, journalists, judges, and military leaders and begins to judge them by the jokes they crack and the diseases they struggle with. Then it will no longer be an independent country but a data colony," Harari said. "In short, technology should not be allowed to be used to collect data for control. However, for bettering each one's lives," he concluded.[22] In one of his articles for *The Atlantic*, Harari argued that artificial intelligence could eliminate the advantages of democracy and undermine the ideals of liberty and equality. Without proper intervention, AI has the potential to concentrate power in the hands of a small elite.

2.2.3. AI and National Security

The widespread popularity of AI is reshaping how countries approach defense and international relations. This section explores AI's impact on national security and its implications for state sovereignty in light of emerging threats. The evolution of AI is altering the landscape of national security, presenting new challenges for states. Technologies like autonomous and cyber weapons provide state and non-state actors with new avenues for influence and power projection. These advancements are revolutionizing defense strategies, with AI bolstering capabilities in border security, enabling better detection and prevention of illicit activities. However, AI's impact on national security challenges traditional concepts of state sovereignty. The proliferation of AI-enabled tools raises concerns about regulating the use of force and safeguarding citizens in an increasingly complex security environment.[23]

---

20 Harari, Y. N. (2016). *Homo Deus: A brief history of tomorrow*. Random House.

21 Harari, Y. N. (2023, April 28). Yuval Noah Harari argues that AI has hacked the operating system of human civilisation. *The Economist*.

22 Harari, 2023.

23 Bryson, Diamantis & Grant, 2017.

Artificial intelligence has emerged as a double-edged sword in security, presenting opportunities and challenges for national sovereignty. On one hand, AI technologies offer powerful tools for enhancing security measures, from predictive analytics to autonomous defense systems, bolstering a nation's ability to protect its citizens and infrastructure. However, the proliferation of AI also poses significant threats to sovereignty.

The possibility of AI-driven cyber-attacks, in which advanced algorithms might compromise a country's stability and control by manipulating data, disrupting communication networks, and taking advantage of weaknesses in vital infrastructure, is one of the main causes of concern. Furthermore, the development of AI-powered autonomous weaponry creates ethical dilemmas and increases the possibility of conflict intensifying beyond human involvement, undermining conventional ideas of sovereignty over military action.[24]

Concerns over accountability and transparency are also raised by using AI algorithms in decision-making processes, such as law enforcement and intelligence gathering. AI system biases have the potential to unintentionally reinforce existing disparities or discriminate against specific groups, undermining the concepts of justice and fairness in sovereign nations.[25]

Automated intelligence analysis has been employed against some Islamic organizations to gather information and spot hostile actions for targeting.[26] Robust investments in research and development by the USA further underscore the importance of a military with enhanced technology capabilities.[27] US military and political leaders have frequently discussed the Third Offset deterrence policy, which seeks to oppose and defeat China's and Russia's technical advancements and the modernization of their armed forces.[28] The creation of "The Office of Digital and Artificial Intelligence" in February 2022, under the direction of the Chief Officer who manages the development of the US Department of Defense (DoD) and its data, analytics, and AI strategy, further illustrates this focus. Other countries are also actively using AI for military purposes. Russia's AI policy is largely focused on using technology in the defense industry, focusing on robotizing the armed forces through several organizations and conferences. Unmanned ground vehicles with machine guns that can be used for multiple purposes, including warfare, intelligence

---

[24] Simmons-Edler, R., et al. (2024). AI-powered autonomous weapons risk geopolitical instability and threaten AI research. *Proceedings of Machine Learning Research, 235*, 45508–45524.

[25] Peters, U. (2022). Algorithmic political bias in artificial intelligence systems. *Philosophy & Technology, 35*(2), 25.

[26] Department of Defense. (2017). *Memo: Establishment of an Algorithmic Warfare Cross-Functional Team.* Project Maven. (April 26, 2017).

[27] Briscoe, E., & Fairbanks, J. (2020). Artificial scientific intelligence and its impact on national security and foreign policy. *Orbis, 64*(4), 544–554.

[28] Lange, K. (2016, May 31). 3rd offset strategy 101: what it is, what the tech focuses are. *DoD Live*.

gathering, and logistics, are the most well-known programs.[29] Furthermore, the Russian military plans to use AI to make additional vehicles autonomous and advance their swarming capabilities, just like the US and China have done.[30]

3. Comparative BRICS Legal Analysis and Case Studies

3.1. The Legal Challenges of AI to State Sovereignty

Governments and communities worldwide are facing various legal issues due to artificial intelligence. AI-enabled technologies are revolutionizing people's live and work and communicate with each other as they proliferate. Furthermore, AI-driven surveillance technologies enable states to monitor their populations with unprecedented precision, blurring the line between legitimate governance and infringements on individual liberties. Facial recognition, predictive policing algorithms, and social credit systems raise ethical and legal concerns regarding privacy rights and human dignity, challenging the notion of sovereignty as the exclusive domain of state authority. As AI advances and spreads globally, there's a growing recognition of the necessity for global governance to ensure its development and deployment align with ethical and legal standards, safeguarding individuals' human rights.[31] Establishing such governance involves actively engaging diverse stakeholders, including governments, scholars, and civil society organizations.[32] Effective governance ensures that AI development and usage adhere to ethical and legal standards. AI in decision-making processes raises significant concerns about individual privacy protection, as AI-driven algorithms can sometimes display biases against certain groups, leading to discriminatory outcomes.[33]

Furthermore, the deployment of AI technologies like facial recognition and predictive policing raises issues regarding states' capacity to uphold their citizens' privacy and civil liberties.[34] Moreover, the advancement of AI introduces new regulatory challenges for states in overseeing the collection, storage, and utilization of personal data, as AI technologies become increasingly proficient in gathering and analyzing vast amounts of personal information, sparking worries about potential data misuse.

---

[29] Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review, 1*(3), 37–57.

[30] Bendett, S., et al. (2021). *Advanced military technology in Russia*. Chatham House.

[31] Schmitt, L. (2022). Mapping global AI governance: A nascent regime in a fragmented landscape. *AI and Ethics, 2*(2), 303–314.

[32] Erdélyi, O., & Goldsmith, J. (2018). Regulating artificial intelligence: Proposal for a global solution. *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*.

[33] LaBrie, R. C., & Steinke, G. (2019). Towards a framework for ethical audits of AI algorithms. *Americas Conference on Information Systems*.

[34] Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature Medicine, 26*(4), 463–464.

AI presents legal dilemmas highlighting the need for robust legal frameworks to regulate its development and application. Such frameworks ensure that AI operates within ethical and legal boundaries, safeguarding individuals' rights.[35]

These frameworks entail collaboration among various stakeholders, including governments, academics, and civil society organizations. Governments are urged to ensure effective mechanisms are in place to enable cross-border agencies to cooperate and coordinate domestically to identify investigation targets.[36] Despite the intricacies involved, establishing such frameworks is vital to guaranteeing AI's compliance with ethical and legal standards. Governments and societies worldwide grapple with diverse legal challenges stemming from the rise of AI.

3.2. AI in a Changing World

AI has expanded its influence across various domains, including public spaces like political communication, electoral politics, and online political strategies, fundamentally altering the behavior of political actors and regime. Institutions and regimes are no longer insulated from AI-driven politics, raising concerns about sovereignty and democracy.[37] Moreover, AI is increasingly penetrating government policy instruments and digital spaces, giving rise to a new era of political communication on social media platforms.[38]

This profound technological revolution could potentially replace human intervention across society, a vital element for democratic progress.[39] The global competition for AI technology underscores its utility, driving countries to develop policies to harness AI and its applications.[40] This competition impacts sovereignty and

---

[35] Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security, 109*, 102382.

[36] Zali, M., & Maulidi, A. (2018). Fighting against money laundering. *BRICS Law Journal, 5*(3), 40–63.

[37] Kendall-Taylor, A., Frantz, E., & Wright, J. (2020). The digital dictators: How technology strengthens autocracy. *Foreign Affairs, 99*(2), 103–115; Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale Journal of Law & Technology, 21*, 106–188; Wright, N. D. (2019). *Artificial intelligence, China, Russia, and the global order*. Air University Press; Filgueiras, F. (2022). The politics of AI: Democracy and authoritarianism in developing countries. *Journal of Information Technology & Politics, 19*(4), 449–464; Andreeva, E. L. (2026). The problems of information sovereignty in the BRICS countries. *BRICS Law Journal, 13*(1), 76–88.

[38] Filgueiras, F. & Almeida, V. (2020). *Governance for the Digital World: Neither More State nor More Market.* Springer Nature; Jeffares, S. (2020). *The Virtual Public Servant: Artificial Intelligence and Frontline Work*. Springer International Publishing; Pencheva, I., et al. (2020). Big data and AI—A transformational shift for government: So, what next for research? *Public Policy and Administration, 35*(1), 24–44; Filgueiras, 2022; Andreeva, 2026.

[39] Wright, 2019.

[40] Allen, J. R., & Husain, A. (2017). The next space race is artificial intelligence. *Foreign Policy*. https://foreignpolicy.com/2017/11/03/the-next-space-race-is-artificial-intelligence-and-america-is-losing-to-china/; Zeng, J. (2020). Artificial intelligence and China's authoritarian governance. *International Affairs, 96*(6), 1441–1459.

influences power dynamics and global governance.[41] Furthermore, AI's deployment worldwide raises questions about its political neutrality, as the raw data utilized in machine learning is inherently biased, shaping classifications, hierarchies, and decision-making models.[42] Moreover, AI offers authoritarian regimes a means to monitor, understand, and control their citizens more effectively, challenging the dominance of liberal democracy in the global political landscape.[43] This shift could spark renewed international competition between social systems, akin to the struggles between liberal democracy, fascism, and communism in the 20th century. China's development of a digital authoritarian state through surveillance and machine learning exemplifies this trend, potentially leading other countries to adopt similar systems. The historical role of surveillance and data monitoring in economic and social progress has evolved with AI and related technologies, posing risks of authoritarian surveillance-based governance if democratic norms and accountability mechanisms are not reinforced.[44]

Concerns over data protection, privacy, and other principles and values such as equity and equality, autonomy, transparency, accountability, and due process are growing. The dual-use nature of AI applications also makes it difficult to constrain their development and regulate their usage. Moreover, recent public statements by the world leaders such as Chinese President Xi Jinping, Russian President Vladimir Putin, and former US President Donald Trump have highlighted AI as a critical element of national power projection. This trend illustrates that the development and utilization of AI technologies will be increasingly complicated by escalating strategic competition among nations (in geopolitical, military, economic, and normative terms.[45]

Furthermore, it is becoming increasingly evident that some countries aim to use AI as a "critical enabler and force multiplier for capabilities across all aspects of military power."[46] The excessive use of AI may erode key features of democratic politics, such as accountability and responsiveness. These technologies are based on algorithmic systems whose intelligence remains contested and should not be

---

41 Floridi, L. & Cowls, J. (2022). *A Unified Framework of Five Principles for AI in Society*. In Machine Learning and the City: Applications in Architecture and Urban Design, 535–545.

42 Joyce, S. C. (2021). AI as a collaborator in the early stage of the design. In C. Lange & D. Sun (Eds.), *The Routledge companion to artificial intelligence in architecture* (pp. 130–159). Routledge; Gitelman, L. (Ed). (2013). *Raw data is an oxymoron*. MIT Press; Crawford, K. (2021). *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence.* Yale University Press; Filgueiras, 2022.

43 Wright, 2019.

44 Wright, 2019.

45 Kavanagh, C. (2019). *New tech, new threats, and new governance challenges: An opportunity to craft smarter responses?* Carnegie Endowment for International Peace.

46 Vincent, J. (2017). Putin says the nation that leads in AI will be the ruler of the world. *The Verge, 4*(10). https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world; Kavanagh, 2019.

equated with human intelligence.[47] Such technologies interfere with social relations and individual life. AI-based automated systems increasingly operate as artificial agents in society. People in industrialized societies, consciously or unconsciously, rely on filtering algorithms in online searches and social networking sites; to some extent, these systems may be used by governments for algorithmic decision-making without individuals' meaningful control.[48] That is how an individual's choice is altered, violating democratic values and privacy ethics. AI-enabled technologies are creating new forms of power and dominance that may be exercised by state and non-state actors. This is changing patterns of interaction among states.[49]

The advent of AI has changed the sphere of geopolitics and poses a challenge to the autonomy of state sovereignty. The idea of territorial sovereignty is under threat because AI technologies are not bound by places; they could be used from any place in the world.[50] The increasing use of AI is changing the balance of power among states with a significant impact on states' ability to pursue their interests in the international system in the domain of the international system. States that lead in AI development and deployment are likely to gain a significant advantage over those that do not, potentially causing a shift in the power dynamics of the international system.[51]

Predicting the future is difficult given the global nature of AI development. However, in contemporary internet politics, concerns over democracy and democratic values are increasingly present in public debates, and the stability of democracy is being questioned.[52] These concerns relate to technological dominance and its possible connection with the rise of right-wing majoritarianism in Europe and America. The recent rise of AI poses a similar risk: it may gradually undermine democracy and its values, creating conditions that could reshape future political systems.[53]

A notable example of the malicious use of AI involves the creation of online personas, known as social bots, that mimic human behavior. Social bots were intended to promote awareness and foster cooperation among people. However,

---

47 König, P. D., & Wenzelburger, G. (2020). Opportunity for renewal or disruptive force? How artificial intelligence alters democratic politics. *Government Information Quarterly, 37*(3), 101489.

48 Brauneis, R., & Goodman, E. P. (2018). Algorithmic transparency for the smart city. *Yale Journal of Law & Technology, 20*, 103–176.

49 Hudson, V. M. (2019). *Artificial intelligence and international politics*. Routledge.

50 Goode, J. P. (2021). Artificial intelligence and the future of nationalism. *Nations and Nationalism, 27*(2), 363–376.

51 Horowitz, 2018.

52 Sudmann, A. (2019). *The democratization of artificial intelligence: Net politics in the era of learning algorithms*. Transcript.

53 Work, B. (2016, April 28). *Remarks by deputy secretary work on third offset strategy*. US Department of Defense. https://www.war.gov/News/Speeches/Speech/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/

they have frequently been exploited for nefarious purposes, including phishing, fraud, and political manipulation on social networks. Seymour and Tully highlighted that machine learning can be weaponized for social engineering, where AI-driven systems can generate mass-produced messages with phishing links and post them on platforms like Twitter without interruption.[54] Due to the social bots' ability to emulate a specific user's past behavior and public profiles, detecting these malicious bots has become a significant challenge for computer security.[55]

4. AI Legal Framework and Data Sovereignty in BRICS Member States

4.1. Brazil

Each BRICS Member State has a different legal framework for AI governance. In Brazil, data and AI frameworks are primarily provided under the Lei Geral de Proteção de Dados (LGPD) (General Data Protection Law), Law No. 13.709/2018.[56] Article 3 of the LGPD stipulates that this law applies to any data processing regardless of where the entity is located if the activity happens within the country, targets individuals residing there, or involves data collected in Brazil. The Act was modelled after the EU General Data Protection Regulation and contains provisions pertaining to purpose limitation, adequacy, necessity, transparency, security, and accountability.[57] The LGPD also establishes the National Data Protection Authority (ANPD) which functions as the central supervisory authority responsible for enforcement, guidance, and regulatory development.[58]

A key feature of Brazil's data sovereignty framework is Article 33 of the LGPD, which addresses international data transfers. Rather than imposing strict data localization requirements, the LGPD makes cross-border transfers conditional on adequate protection levels or when the controller provides specific legal guarantees, such as standard contractual clauses or binding corporate rules. Alternatively, transfers are allowed for specific legal necessities, including protecting an individual's life, fulfilling international cooperation agreements, or obtaining the data subject's explicit and

---

54 Seymour, J., & Tully, Ph. (2016). Weaponising data science for social engineering: Automated E2E spear phishing on Twitter. *Black Hat USA, 37*, 1–39.

55 Shi, L., et al. (2024). Enhancing social cohesion with cooperative bots in societies of greedy, mobile individuals. *PNAS Nexus*.

56 de Freitas Júnior, A. R., Zapolla, L. F., & Cunha, P. F. N. (2024). The regulation of artificial intelligence in Brazil. *ILR Review, 77*(5), 869–878.

57 Gadoni, C. R. (2023). The effects on local innovation arising from replicating the GDPR into the Brazilian General Data Protection Law. *Internet Policy Review, 12*(1), 1–22.

58 Luz, J. C. J. (2025). Role of data protection authorities in Nigeria (NDPC) and Brazil (ANPD). *NDPC – International Journal of Data Privacy and Protection*, 156–170.

informed consent.[59] This approach allows Brazil to participate in global digital markets while ensuring that Brazilian data exported abroad remains subject to protective standards aligned with domestic law. Sovereignty is expressed not through territorial isolation of data, but through regulatory leverage where multinational platforms must comply with Brazilian standards.[60]

Beyond data protection, Brazil has developed broader AI governance strategies. In 2021, the government adopted the Estratégia Brasileira de Inteligência Artificial (EBIA) (Brazilian Artificial Intelligence Strategy). EBIA outlines principles such as ethical use, transparency, human-centric development, innovation promotion, and international cooperation. While it is largely strategic and programmatic rather than binding, EBIA signaled Brazil's intention to position itself as both an AI innovator and a responsible regulator.[61] More recently, Brazil introduced the Plano Brasileiro de Inteligência Artificial (PBIA) (Brazilian Artificial Intelligence Plan) 2024–2028, branded as "AI for the Good of All." This plan emphasizes national technological capacity, public-sector digital transformation, and strategic autonomy in data infrastructure and computing resources. From a sovereignty perspective, PBIA reflects an understanding that effective control over AI systems requires not only regulatory safeguards but also domestic capability in data governance, cloud infrastructure, and research ecosystems.[62]

On the legislative front, on 10 December 2024, the Brazilian Senate approved the Artificial Intelligence Act (Bill No. 2338/2023). The Bill is pending in the Chamber of Deputies for a vote before the President can sign it into law. It aims to establish operational guidelines and requirements, protect human rights and provide penalties for non-compliance. It takes a risk-based approach to regulating AI systems by placing stricter rules on high-risk systems, especially those that could affect public safety or fundamental human rights. It also requires AI developers and users to make their systems fair, transparent, and easy to understand.[63]

---

59 Rajagopalan, A. S. (2021). International personal data transfer: An analysis of Brazil's legal system and new LGPD under the adequacy standard of the EU GDPR. *Journal of Data Protection & Privacy, 4*(3), 260–272.

60 Belli, L., & Doneda, D. (2023). Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. *International Data Privacy Law, 13*(1), 1–24.

61 Filgueiras, F., & Junquilho, T. A. (2023). The Brazilian (non)perspective on national strategy for artificial intelligence. *Discover Artificial Intelligence, 3*(7); Neto, G. P. J., Farias da Costa, V. C., & Gaspar, W. B. (2024). Brazil's Artificial Intelligence Plan (PBIA) of 2024: Enabler of AI sovereignty? *African Journal of Information and Communication, 2024*(34), 1–15.

62 Filgueiras & Junquilho, 2023; Neto, Farias da Costa & Gaspar, 2024.

63 Mendes, L. S., & Kira, B. (2025). Brussels to Brasilia: Brazil's distinct path in AI regulation. In S. Simitis & I. Spiecker genannt Döhmann (Eds.), *Digital Constitutionalism* (pp. 345–364). Nomos.

4.2. Russia

Russia's approach to AI and data sovereignty reflects a strong system of state supervision. It also focuses on experimental regulation within controlled environments and alignment of AI development with national technological sovereignty and security priorities. Federal Law of July 27, 2006 No. 152-FZ "On Personal Data" establishes the framework for processing personal data.[64] Specifically, Article 18(5) requires that the recording, systematization, accumulation, storage, clarification, and retrieval of personal data of Russian citizens be carried out using databases located within the territory of the Russian Federation. Russia uses a "data localization" approach in protecting the personal data of its citizens.[65] Cross-border transfer of personal data is further regulated under Articles 12 and 12.1, which require an assessment of whether the receiving state provides adequate protection of data subjects' rights.[66] Enforcement authority lies with the Federal Service for Supervision of Communications, Information Technology and Mass Media, which has the power to block non-compliant services.[67]

Russia also treats digital sovereignty as a matter of national security. The Federal Law of July 27, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection" provides the general legal regime for information governance, including obligations on information system operators and powers to restrict access to unlawful content.[68] Additionally, the Doctrine of Information Security of the Russian Federation (2016) and the National Security Strategy of the Russian Federation (2021) explicitly characterize information and digital technologies as strategic domains requiring state protection against external influence.[69] Specifically on AI, Russia adopted the National Strategy for the Development of Artificial Intelligence for the Period up to 2030, approved by Presidential Decree of October 10, 2019 No. 490.[70] The Strategy defines AI, sets national objectives for research, commercialization, and public-sector deployment, and highlights the importance of regulatory adaptation.

---

64 Egorova, T. (2013). Personal Data Legislation in Russia. *International. In-House Counsel Journal*, 7, 1.

65 Khasanova, L., & Tai, K. (2023). An Authoritarian Approach to Digital Sovereignty? Russian and Chinese Data Localization Models. Russian and Chinese Data Localization Models (July 31, 2023). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4527052

66 Bakhteev, D. V., Sosnovikova, A. M., & Kazenas, E. V. (2024). Overcoming illegal cross-border transfer of personal data. *Journal of Digital Technologies and Law, 2*(4), 943–972.

67 Haworth, L. (2018). The latest wave of internet blocking in Russia—what's behind it and if it matters. *Gaming Law Review, 22*(1), 31–39.

68 Pushkarev, V., & Solomatina, A. (2025). Computer information crimes and other cybercrimes: Comparative legal analysis of the legislation of the BRICS countries. *BRICS Law Journal, 12*(4), 167–190.

69 Hancock, B., et al. (2025). Understanding Russia's cyber policies, strategies, and doctrines. *Military Cyber Affairs, 8*(1), 1–26.

70 Neznamov, A. V., Chache, E. G., & Churilova, D. Y. (2025). What is "regulatory path" for Russia? *Legal Issues in the Digital Age, 6*(3), 4–22.

It calls for the development of legal mechanisms addressing ethical standards, safety, and responsibility in AI.[71]

4.3. India

India adopts a state-centric yet innovation-oriented approach to AI and data sovereignty. It combines executive control over cross-border data flows, security-driven digital governance under the IT framework, and policy-led development of responsible and inclusive artificial intelligence. The Digital Personal Data Protection Act 2023 (DPDP Act) establishes a comprehensive framework for the processing of "digital personal data." Section 3 stipulates that the Act shall apply to entities processing data within India, as well as to processing outside India where goods or services are offered to individuals in India.[72] Under Section 16, the Central Government may, by notification, restrict transfers of personal data to specific countries or territories. In the absence of such a restriction, transfers are generally permitted.[73] This reflects a sovereignty model based on executive control over outbound data flows rather than blanket localization. Chapter V of the DPDP Act establishes the Data Protection Board of India, which is empowered to adjudicate non-compliance and enforce penalties, as well as to oversee both domestic and foreign technology companies operating in India.[74]

The Information Technology Act 2000 (IT Act) provides a framework for digital governance of electronic data and cybersecurity.[75] Section 43A imposes liability on bodies corporate for failure to protect sensitive personal data, while Section 69A empowers the Central Government to block public access to information in the interest of sovereignty, integrity, defense, and security of the state. Regarding AI, rather than relying on legislation, India's governance is based on policy guidance through the National Strategy for Artificial Intelligence (2018), titled "AI for All" and the "Responsible AI for All" discussion paper (2021).[76] The strategy emphasizes inclusive growth, sectoral deployment (health, agriculture, education, smart mobility), and responsible AI principles. Meanwhile, the discussion paper outlines principles such as safety, reliability, equality, transparency, and accountability. In 2023, the Ministry

---

[71] Kozyulin, V. (2023). Assessing Russia's national strategy for AI development. In M. Raska & R. A. Bitzinger (Eds.), *The AI wave in defence innovation* (pp. 156–178). Routledge.

[72] Naithani, P. (2025). Analysis of India's Digital Personal Data Protection Act, 2023. *International Journal of Law and Management, 67*(5), 543–553.

[73] Singh, S. (2024). Regulation of cross-border data flow and its privacy in the digital era. *NUJS Journal of Regulatory Studies, 9*, 38.

[74] Vidya, M. N. (2025). *Data Protection in the Era of Digitization: with Special Reference to Data Privacy and Data Localization in India* (Doctoral dissertation). Alliance University, India.

[75] Madhusudan, V. V. (2024). A critical analysis of Information Technology Act, 2000 with reference to cyber offence and cyber security. *International Journal of Law Management & Humanities, 7*(2), 25–29.

[76] Kathuria, Y., et al. (2024). Responsible AI impact assessment mechanism for India: A robust strategy for effective governance of AI systems in the country. *AIP Conference Proceedings*, *3220*(1), 040010.

of Electronics and Information Technology issued the advisory requiring AI platforms to ensure due diligence and prevent harmful or unlawful outputs, reinforcing a regulatory expectation that AI deployment must align with constitutional values, public order, and national sovereignty.[77]

4.4. China

China adopts a state-centric and security-driven model of AI and data sovereignty that combines strict data governance laws, localization and export controls, and targeted regulation of algorithmic systems to ensure alignment with national security, social stability, and state policy objectives. Data sovereignty is regulated under three main statutes: the Cybersecurity Law of the People's Republic of China (2017), the Data Security Law (DSL) (2021), and the Personal Information Protection Law (PIPL) (2021).[78] Article 37 of the Cybersecurity Law requires operators of critical information infrastructure (CII) to store personal information and important data collected within China domestically, unless security assessment conditions for cross-border transfer are satisfied. Meanwhile, the Data Security Law further strengthens sovereign control by establishing a classification and graded protection system for data (Arts. 21–23) and introducing national security-based restrictions on data export (Art. 31). The PIPL 2021 regulates the processing of personal information and imposes strict conditions on cross-border transfers under Articles 38–43, including government-administered security assessments, certification, or standard contracts.[79]

On AI governance, China has moved decisively toward sector-specific regulatory instruments. The Provisions on the Administration of Algorithmic Recommendation in Internet Information Services (2022) require algorithmic recommendation service providers to promote "positive energy," avoid endangering national security or social order, and register certain algorithms with the authorities (Arts. 4 and 24).[80] This was followed by the Interim Measures for the Management of Generative Artificial Intelligence Services (2023), jointly issued by the Cyberspace Administration of China and other ministries. The Interim Measures require generative AI providers to ensure that training data and outputs comply with laws and socialist core values (Art. 4), prevent discrimination (Art. 7), and conduct security assessments where services influence public opinion or have the capacity for social mobilization.[81] These instruments

---

77 Advisory No. 2(4)/2023-CyberLaws, December 26, 2023 (India).

78 Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity, 8*(1), 1–12.

79 Yi-Chen, Z. (2025). China's Personal Information Protection Law (PIPL) 2021: An analysis. *Modern Jurisprudence, 3*(3).

80 Yang, F., & Yao, Y. (2022). A new regulatory framework for algorithm-powered recommendation services in China. *Nature Machine Intelligence, 4*(10), 802–803.

81 Migliorini, S. (2024). China's interim measures on generative AI: Origin, content and significance. *Computer Law & Security Review, 53*, 105985.

demonstrate that China's AI governance is not merely about innovation policy, but about embedding algorithmic systems within a broader framework of ideological supervision, cybersecurity control, and sovereign data governance.[82]

Conclusion

Thus, it can be seen that AI presents a disturbing outlook in relation to state sovereignty. Case studies such as AI surveillance, autonomous weapons, cyberattacks, data sovereignty, BRICS legal frameworks illustrate the complex interplay between AI and state sovereignty. As AI advances and human consciousness evolves, the traditional Westphalian model of sovereignty based on territoriality and exclusivity may give way to a more fluid and networked conception of governance. The rapid growth of AI has a long-lasting impact on the security of the nation and the global economy. Increasing "dataism" and the expanding reach of AI into revolutionary technologies and human consciousness have hampered various aspects of individual and state sovereignty. Legal challenges concerning the control and protection of data are also among the biggest challenges of the modern world, living with AI. Global politics and national security are also affected by the challenges posed by AI worldwide. Looking ahead, policymakers will need to navigate these challenges by adopting flexible and adaptive approaches to sovereignty that accommodate the realities of a rapidly changing world. This may involve rethinking traditional notions of jurisdiction, authority, and legitimacy in light of emerging technologies and evolving human values. Ultimately, the future of state sovereignty in the age of AI and changing consciousness will depend on the ability of states and international institutions to address complexity, foster dialogue, and forge inclusive governance structures that reflect humanity's diverse needs and aspirations.

References

Allen, J. R., & Husain, A. (2017). The next space race is artificial intelligence. *Foreign Policy*. https://foreignpolicy.com/2017/11/03/the-next-space-race-is-artificial-intelligence-and-america-is-losing-to-china/

Andreeva, E. L. (2026). The problems of information sovereignty in the BRICS countries. *BRICS Law Journal, 13*(1), 76–88. https://doi.org/10.21684/2412-2343-2026-13-1-76-88

Aydın, A., & Bensghir, T. K. (2019). Digital data sovereignty: Towards a conceptual framework. In *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, 1–6. https://doi.org/10.1109/ubmyk48245.2019.8965469

[82] Zhao, S. (Ed.). (2025). *The making of China's artificial intelligence and cyber security policy: Players, governance, and global ambition*. Taylor & Francis.

Bakhteev, D. V., Sosnovikova, A. M., & Kazenas, E. V. (2024). Overcoming illegal cross-border transfer of personal data. *Journal of Digital Technologies and Law, 2*(4), 943–972. https://doi.org/10.21202/jdtl.2024.45

Belli, L., & Doneda, D. (2023). Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. *International Data Privacy Law, 13*(1), 1–24. https://doi.org/10.1093/idpl/ipac019

Bendett, S., et al. (2021). *Advanced military technology in Russia*. Chatham House.

Bodin, J. (1992). *On sovereignty: Four chapters from the six books of the commonwealth*. Cambridge University Press.

Brauneis, R., & Goodman, E. P. (2018). Algorithmic transparency for the smart city. *Yale Journal of Law & Technology, 20*, 103–176. https://doi.org/10.2139/ssrn.3012499

Briscoe, E., & Fairbanks, J. (2020). Artificial scientific intelligence and its impact on national security and foreign policy. *Orbis, 64*(4), 544–554. https://doi.org/10.1016/j.orbis.2020.08.004

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law, 25*, 273–291. https://doi.org/10.1007/s10506-017-9214-9

Couture, S., & Toupin, S. (2017). *What does the concept of sovereignty mean in digital, network and technological sovereignty?* GigaNet: Global Internet Governance Academic Network, Annual Symposium. https://doi.org/10.2139/ssrn.3107272

Crawford, K. (2021). *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press. https://doi.org/10.2307/j.ctv1ghv45t

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity, 8*(1), 1–12. https://doi.org/10.1093/cybsec/tyac01

de Freitas Júnior, A. R., Zapolla, L. F., & Cunha, P. F. N. (2024). The regulation of artificial intelligence in Brazil. *ILR Review, 77*(5), 869–878. https://doi.org/10.1177/00197939241278956g

Egorova, T. (2013). Personal data legislation in Russia. *International In-House Counsel Journal, 7*(26), 1–16.

Erdélyi, O., & Goldsmith, J. (2018). Regulating artificial intelligence: Proposal for a global solution. *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*. https://doi.org/10.1145/3278721.3278731

Filgueiras, F. (2022). The politics of AI: Democracy and authoritarianism in developing countries. *Journal of Information Technology & Politics, 19*(4), 449–464. https://doi.org/10.1080/19331681.2021.2016543

Filgueiras, F., & Junquilho, T. A. (2023). The Brazilian (non)perspective on national strategy for artificial intelligence. *Discover Artificial Intelligence, 3*(7). https://doi.org/10.1007/s44163-023-00052-w

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security, 109*, 102382. https://doi.org/10.1016/j.cose.2021.102382

Gadoni, C. R. (2023). The effects on local innovation arising from replicating the GDPR into the Brazilian General Data Protection Law. *Internet Policy Review, 12*(1), 1–22. https://doi.org/10.14763/2023.1.1686

Gitelman, L. (Ed). (2013). *Raw data is an oxymoron*. MIT Press. https://doi.org/10.7551/mitpress/9302.001.0001

Goode, J. P. (2021). Artificial intelligence and the future of nationalism. *Nations and Nationalism, 27*(2), 363–376. https://doi.org/10.1111/nana.12684

Grittersová, J. (1999). The evolution of the concept and the role of sovereignty. *Medzinárodné otázky*, 105–117.

Hancock, B., et al. (2025). Understanding Russia's cyber policies, strategies, and doctrines. *Military Cyber Affairs, 8*(1), 1–26.

Harari, Y. N. (2016). *Homo Deus: A brief history of tomorrow*. Random House.

Harari, Y. N. (2023, April 28). Yuval Noah Harari argues that AI has hacked the operating system of human civilisation. *The Economist*.

Haworth, L. (2018). The latest wave of internet blocking in Russia—what's behind it and if it matters. *Gaming Law Review, 22*(1), 31–39. https://doi.org/10.1089/glr2.2018.2215

Henkin, L. (1995). Human rights and state sovereignty. *Georgia Journal of International and Comparative Law, 25*, 31–46.

Hobbes, T. (1968). *Leviathan*. Penguin Books.

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review, 1*(3), 37–57.

Hudson, V. M. (2019). *Artificial intelligence and international politics*. Routledge. https://doi.org/10.4324/9780429033575

Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature Medicine, 26*(4), 463–464. https://doi.org/10.1038/s41591-020-0832-5

Joyce, S. C. (2021). AI as a collaborator in the early stage of the design. In C. Lange & D. Sun (Eds.), *The Routledge companion to artificial intelligence in architecture* (pp. 130–159). Routledge. https://doi.org/10.4324/9780367824259-9

Kathuria, Y., et al. (2024). Responsible AI impact assessment mechanism for India: A robust strategy for effective governance of AI systems in the country. *AIP Conference Proceedings*, *3220*(1), 040010. https://doi.org/10.1063/5.0234670

Kavanagh, C. (2019). *New tech, new threats, and new governance challenges: An opportunity to craft smarter responses?* Carnegie Endowment for International Peace.

Kello, L. (2023) The state in the digital era. In *Digital international relations* (pp. 51–72). Taylor & Francis. https://doi.org/10.4324/9781003437963-4

Kendall-Taylor, A., Frantz, E., & Wright, J. (2020). The digital dictators: How technology strengthens autocracy. *Foreign Affairs, 99*(2), 103–115.

König, P. D., & Wenzelburger, G. (2020). Opportunity for renewal or disruptive force? How artificial intelligence alters democratic politics. *Government Information Quarterly, 37*(3), 101489. https://doi.org/10.1016/j.giq.2020.101489

Kozyulin, V. (2023). Assessing Russia's national strategy for AI development. In M. Raska & R. A. Bitzinger (Eds.), *The AI wave in defence innovation* (pp. 156–178). Routledge. https://doi.org/10.4324/9781003218326-8

LaBrie, R. C., & Steinke, G. (2019). Towards a framework for ethical audits of AI algorithms. *Americas Conference on Information Systems*.

Lange, K. (2016, May 31). 3rd offset strategy 101: what it is, what the tech focuses are. *DoD Live*.

Luz, J. C. J. (2025). Role of data protection authorities in Nigeria (NDPC) and Brazil (ANPD). *NDPC – International Journal of Data Privacy and Protection*, 156–170.

Madhusudan, V. V. (2024). A critical analysis of Information Technology Act, 2000 with reference to cyber offence and cyber security. *International Journal of Law Management & Humanities, 7*(2), 25–29.

Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale Journal of Law & Technology, 21*, 106–188.

Mendes, L. S., & Kira, B. (2025). Brussels to Brasilia: Brazil's distinct path in AI regulation. In S. Simitis & I. Spiecker genannt Döhmann (Eds.), *Digital Constitutionalism* (pp. 345–364). Nomos. https://doi.org/10.5771/9783748938644-345

Migliorini, S. (2024). China's interim measures on generative AI: Origin, content and significance. *Computer Law & Security Review, 53*, 105985. https://doi.org/10.1016/j.clsr.2024.105985

Naithani, P. (2025). Analysis of India's Digital Personal Data Protection Act, 2023. *International Journal of Law and Management, 67*(5), 543–553. https://doi.org/10.1108/ijlma-05-2024-0174

Neto, G. P. J., Farias da Costa, V. C., & Gaspar, W. B. (2024). Brazil's Artificial Intelligence Plan (PBIA) of 2024: Enabler of AI sovereignty? *African Journal of Information and Communication, 2024*(34), 1–15. https://doi.org/10.23962/ajic.i34.20424

Neznamov, A. V., Chache, E. G., & Churilova, D. Y. (2025). What is "regulatory path" for Russia? *Legal Issues in the Digital Age, 6*(3), 4–22. https://doi.org/10.17323/2713-2749.2025.3.4.22

Pencheva, I., et al. (2020). Big data and AI—A transformational shift for government: So, what next for research? *Public Policy and Administration, 35*(1), 24–44. https://doi.org/10.1177/0952076718780537

Peters, U. (2022). Algorithmic political bias in artificial intelligence systems. *Philosophy & Technology, 35*(2), article number 25. https://doi.org/10.1007/s13347-022-00512-8

Philpott, D. (1999). Westphalia, authority, and international society. *Political Studies, 47*(3), 566–589. https://doi.org/10.1111/1467-9248.00217

Philpott, D. (2001). Usurping the sovereignty of sovereignty? *World Politics, 53*(2), 297–324. https://doi.org/10.1353/wp.2001.0006

Philpott, D. (2016). Sovereignty. In E. N. Zalta (Ed.). *The Stanford encyclopedia of philosophy*. Metaphysics Research Lab, Stanford University.

Pushkarev, V., & Solomatina, A. (2025). Computer information crimes and other cybercrimes: Comparative legal analysis of the legislation of the BRICS countries. *BRICS Law Journal, 12*(4), 167–190. https://doi.org/10.21684/2412-2343-2025-12-4-167-190

Rajagopalan, A. S. (2021). International personal data transfer: An analysis of Brazil's legal system and new LGPD under the adequacy standard of the EU GDPR. *Journal of Data Protection & Privacy, 4*(3), 260–272. https://doi.org/10.69554/msqx9692

Schmitt, L. (2022). Mapping global AI governance: A nascent regime in a fragmented landscape. *AI and Ethics, 2*(2), 303–314. https://doi.org/10.1007/s43681-021-00083-y

Seymour, J., & Tully, Ph. (2016). Weaponising data science for social engineering: Automated E2E spear phishing on Twitter. *Black Hat USA, 37*, 1–39.

Shi, L., et al. (2024). Enhancing social cohesion with cooperative bots in societies of greedy, mobile individuals. *PNAS Nexus*. https://doi.org/10.1073/pnasnexus.pgae223

Simmons-Edler, R., et al. (2024). AI-powered autonomous weapons risk geopolitical instability and threaten AI research. *Proceedings of Machine Learning Research, 235*, 45508–45524. https://arxiv.org/abs/2405.01859

Singh, S. (2024). Regulation of cross-border data flow and its privacy in the digital era. *NUJS Journal of Regulatory Studies, 9*, 38. https://doi.org/10.69953/njrs.v9i2.9

Sørensen, G. (1999). Sovereignty: Change and continuity in a fundamental institution. *Political Studies, 47*(3), 590–604. https://doi.org/10.1111/1467-9248.00218

Sudmann, A. (2019). *The democratization of artificial intelligence: Net politics in the era of learning algorithms*. Transcript.

Timmers, P. (2019). Ethics of AI and cybersecurity when sovereignty is at stake. *Minds and Machines, 29*(4), 635–645. https://doi.org/10.1007/s11023-019-09508-4

Usman, H., Nawaz, B., & Nasser, S. (2023). The future of state sovereignty in the age of artificial intelligence. *Journal of Law & Social Studies, 5*(2), 142–152. https://doi.org/10.52279/jlss.05.02.142152

Vincent, J. (2017). Putin says the nation that leads in AI will be the ruler of the world. *The Verge, 4*(10). https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world.

Work, B. (2016, April 28). *Remarks by deputy secretary work on third offset strategy*. US Department of Defense. https://www.war.gov/News/Speeches/Speech/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/

Wright, N. D. (2019). *Artificial intelligence, China, Russia, and the global order*. Air University Press.

Yang, F., & Yao, Y. (2022). A new regulatory framework for algorithm-powered recommendation services in China. *Nature Machine Intelligence, 4*(10), 802–803. https://doi.org/10.1038/s42256-022-00546-9

Yi-Chen, Z. (2025). China's Personal Information Protection Law (PIPL) 2021: An analysis. *Modern Jurisprudence, 3*(3).

Zeng, J. (2020). Artificial intelligence and China's authoritarian governance. *International Affairs, 96*(6), 1441–1459.

Zhao, S. (Ed.). (2025). *The making of China's artificial intelligence and cyber security policy: Players, governance, and global ambition*. Taylor & Francis. https://doi.org/10.4324/9781003627654

Information about the authors

Saslina Kamaruddin (Tashkent, Uzbekistan) – Research Fellow, Central Asian Legal Research Centre, Tashkent State University of Law (35 Sayilgokh St., Tashkent, 100047, Uzbekistan); PhD, Senior Lecturer, Department of Business Management and Entrepreneurship, Sultan Idris Education University (UPSI) (Tanjung Malim, Perak, 35900, Malaysia; e-mail: saslina@fpe.upsi.edu.my) – **corresponding author**.

Muhammad Izwan Ikhsan (Kota Kinabalu, Malaysia) – BLS (Hons), LLB (Hons), LLM Lecturer, Department of Law, MARA University of Technology (Universiti Teknologi MARA (UiTM)) (Beg Berkunci 71, Kota Kinabalu, Sabah, 88997, Malaysia; e-mail: izwanikhsan@uitm.edu.my).

Navtika Singh Nautiyal (Gandhinagar, India) – PhD, Assistant Professor, Forensic Justice and Policy Studies Department, National Forensic Sciences University (Sector-9, Gandhinagar, Gujarat, 382007, India; e-mail: Navtika.nautiyal@nfsu.ac.in).