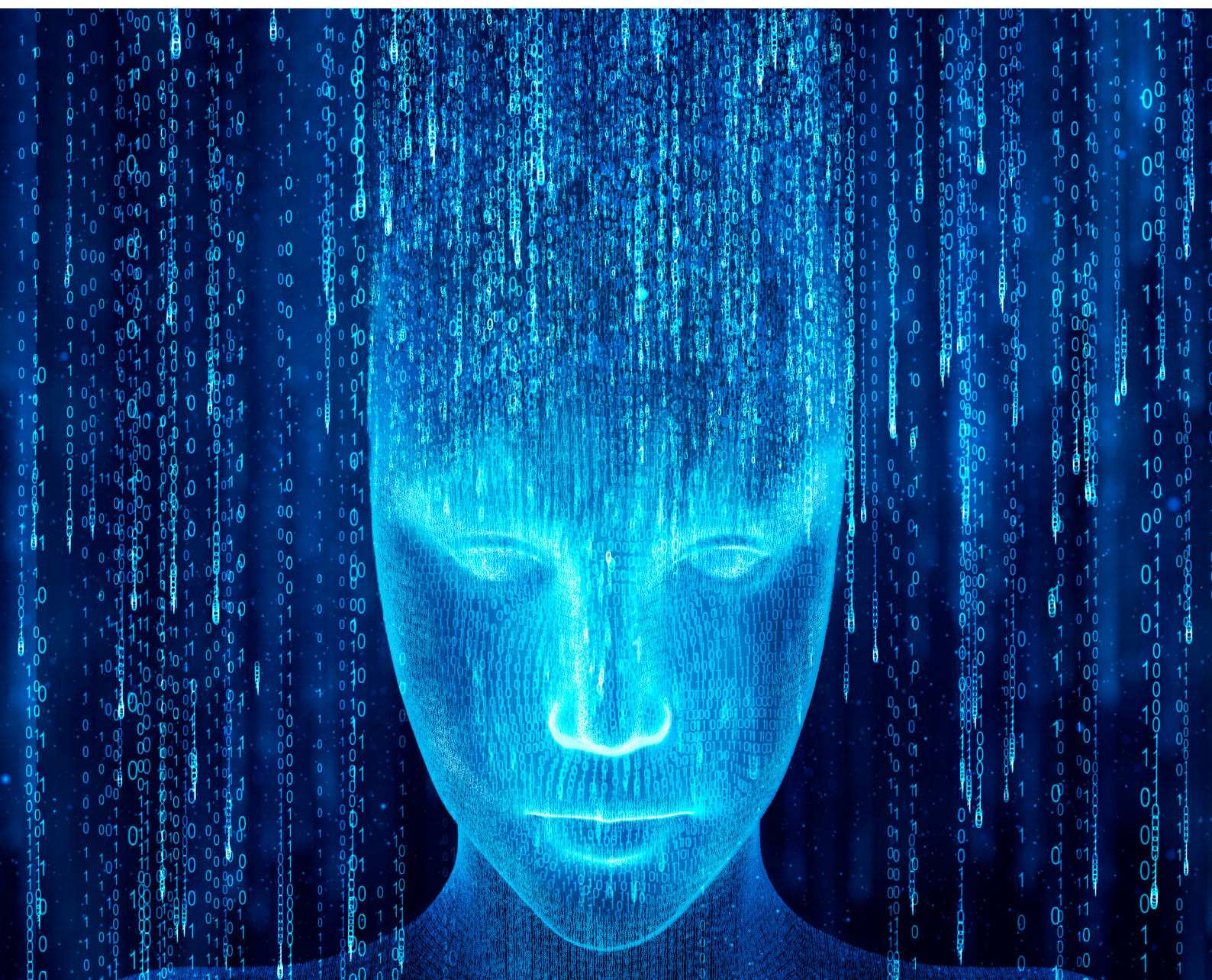# AI Governance in India: Aspirations and Apprehensions

Pranjal Sharma, Anirban Sarma,
Amoha Basrur, Prateek Tripathi

Abstract

The Observer Research Foundation's first Tech Huddle was held on 23 November 2023 and focused on the governance of artificial intelligence (AI) in India, highlighting the rapid growth and adoption of AI as well as the complexities associated with developing regulatory frameworks for it. AI governance is in its infancy, both globally and in India, and grapples with issues such as the explainability of AI systems as well as the embedded biases, safety, security, and accountability of these systems. There are calls for the increased regulation of AI from governments, industry, and civil society. This report traces India's experiences and challenges in characterising, governing, and strengthening AI ecosystems; emphasises the importance of a multistakeholder approach in AI development, with appropriate guardrails and human involvement; and underscores the need for responsible and ethical AI innovation.

Introduction

On 23 November 2023, the Observer Research Foundation hosted the first roundtable under its Tech Huddle[a] event series. The theme of the Huddle was "AI Governance in India: Aspirations and Apprehensions". The event focused on emerging opportunities and challenges around artificial intelligence (AI), the development of related governance frameworks, and strengthening the AI ecosystem in India. The Huddle brought together 25 representatives from business and industry, thinktanks, and academia.

The world is currently undergoing an "AI spring".[1] Major strides in the development of AI algorithms and techniques and an exponential increase in computing power and the volume of available data across sectors are driving significant advances. Nearly 77 percent of all digital devices today use AI.[2] There has been a surge in investments in AI startups in 2023 alone, with a marked spike in interest in generative AI.[3] The global AI market is expected to touch US$191 billion by 2025, at a compound annual growth rate (CAGR) of 36.62 percent. Additionally, AI is expected to add US$15.7 trillion to the world's GDP by 2030, boosting it by 14 percent.[4]

Despite the rapid progress of AI, efforts to govern and regulate it are in a nascent stage. There are growing concerns about this gap, and AI governance frameworks worldwide are striving to address multiple challenges, including systematically evolving explainability standards and elucidating the methodologies of AI systems in order to boost trust and confidence in these systems. Unjust biases embedded in algorithmic systems could have damaging consequences for

---

a   The Tech Huddle is a quarterly curated conversation hosted by ORF dedicated to fostering topical discussions among key stakeholders in the technology ecosystem. These sessions bring together experts to deliberate on critical issues and emerging trends within the global and Indian technology landscape.

access to services or social cohesion and need to be prevented. Further, the safety and security of AI should be strengthened. Human–AI collaboration also needs to be considered with a view to introduce human agents at strategic points within otherwise automated systems. Finally, the liability and accountability of organisations and individuals that build AI need to be better understood.[5]

Recognising some of these issues, the G20, during India's presidency, agreed on the need to "pursue a pro-innovation regulatory/governance approach that maximises the benefits and takes into account the risks associated with the use of AI".[6] Concerns about AI governance also served as the impetus for the United Nations (UN) to set up an AI Advisory Body in October 2023.[7] The subject is also likely to be a focus of the Global Partnership on AI (GPAI) Summit that is being hosted by India in December 2023.

Although India is yet to develop a consolidated national AI governance mechanism, several initiatives and guidelines have been established. NITI Aayog's "National Strategy for AI" (2018) was a foundational document, and some of its recommendations are already in the process of being implemented.[8] NITI Aayog has also developed a roadmap for building a responsible and ethical AI ecosystem.[9] The India Datasets platform aims to provide access to a vast corpus of anonymised public and private datasets in order to facilitate the training of AI models.[10] In August 2023, Microsoft's *Governing AI: A Blueprint for India* report outlined a five-point approach for the public governance of AI.[11]

Characterising AI

The concept of AI dates to the 1950s. Alan Turing's[b] inquiries into the possibility of machines using information and reason to solve problems in the same way as humans formed the basis of his paper, "Computing Machinery and Intelligence" (1950), which explored how to build intelligent machines and test their intelligence. A proof of concept—called the Logic Theorist—was subsequently presented at the Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI) in 1956 and is widely considered to be the first AI programme.[12]

The development of machine learning (ML) as a subset of AI in the 1990s allowed machines to learn independently, without human intervention, through ingesting large volumes of data and detecting patterns. Deep learning, which has gained significant traction since 2012, is a subset of ML and is based on the idea of neural networks, making use of "layers of information processing, each gradually learning more and more complex representations of data".[13]

Generative AI—which are deep learning models that can generate high-quality text, images, and other types of content based on their training data—has democratised AI to make it accessible to every individual and initiated an almost 'interpersonal' way of interacting with AI. Generative AI is extendable to nearly every domain and could be especially invaluable for small and medium enterprises (SMEs). However, generative AI could have disturbing legal and social implications. It raises questions about the safety of intellectual property and data security as well as the prevention of social biases against certain groups or communities. These risks underline the importance of instituting robust AI governance mechanisms and AI regulation. Recent statements and declarations by multilateral bodies and international groups, including

---

b   Alan Turing was a British mathematician, logician, and computer scientist known for laying the foundations for modern computer science.

the G7, the G20, the Organisation for Economic Cooperation and Development (OECD), and the nations attending the AI Safety Summit at Bletchley Park in November 2023, have pushed for collaborative AI development while urging that the "protection of human rights, transparency and explainability, fairness, accountability, regulation, safety, appropriate human oversight, ethics, bias mitigation, privacy and data protection need to be addressed".[14]

It is important to identify the parts of AI that need to be regulated. Additional questions that need to be addressed include whether AI as a whole needs to be regulated or it should be broken down by use cases and overseen by sectoral regulations. An alternative approach could be to categorise risks and formulate regulations for them. There is also a need to examine the AI tech stack and consider how to regulate its different layers. For example, the data infrastructure that serves as the stack base could remain relatively open, while large language models are regulated. At the front end, which includes application programming interfaces (APIs), high-risk, medium-risk, and low-risk situations need to be defined and regulatory measures adopted accordingly. New laws are not necessary since the introduction of human interventions in high-risk situations could sometimes defuse risks. However, excessive harmonisation of approaches and standards around AI could result in specific contexts not being adequately recognised. Therefore, issues such as AI bias need to be contextualised for India and other countries of the Global South.

A regulatory regime that is somewhat akin to licensing regimes could be valuable. For example, the Ministry of Electronics and IT follows an empanelment process for cloud service providers that defines a base-level standard for them at the beginning. A similar predefined layer or standard for hosting data foundations could be useful. For instance, a stringent 'KY3C' framework—know your customer, content, and cloud—could mitigate some of the risks posed by AI. Additionally, there is a need for guardrails and a risk-based approach to AI output. This might also entail the need for a 'co-pilot'—an individual who can check the accuracy and meaning of an AI system's output.

Governing AI

While India's stance on AI regulation has sometimes appeared to waver,[15] it is steadily working towards establishing a clear regulatory approach and AI governance mechanism, especially as the country assumes a more prominent role in the area of AI-related international cooperation.[16]

AI-enabled harms and security threats exist at all three levels of the AI stack: At the hardware level, there are vulnerabilities in the physical infrastructure of AI systems. At a foundational model level, there are concerns around the use of inappropriate datasets, data poisoning, and issues related to data collection, storage, and consent. At the application level, there are threats to sensitive and confidential information as well as the proliferation of capability-enhancing tools among malicious actors. Therefore, while the governance of the tech stack is a priority, governance of the organisations developing AI solutions, or the people behind the technology, could also be productive.

Even as democratisation has made AI more accessible, assigning responsibility and defining accountability for the operation of AI systems have become more difficult. There are ongoing debates about who is responsible for the harms emanating from AI,[17] but it is clear that there is a need for a multistakeholder approach that includes guardrails at the levels of the developer, deployer, and user. It is also necessary to recognise that the nature and use of AI as a technology is different from the harnessing of nuclear energy or electricity, which contain elements of predictability that allow safeguards. On the other hand, AI, especially evolving models of artificial general intelligence (AGI) that are still under development, is unpredictable.[18]

AI development needs to prioritise trust from both users and regulators. Two key methods for building trust are disclosures and detection mechanisms. Disclosure guidelines for developers and deployers would be a significant step towards achieving transparency in AI. Disclosures should include information about the purpose of algorithms, the training data used, and potential biases and risks. Generative AI models should also be accompanied by a detection mechanism. However, since present detection mechanisms may not be adequate for identifying the provenance of content, alternative methods such as watermarking AI-generated content, need to be mainstreamed. Higher standards for disclosure and detection should be applied to dual-use foundational models that have versatile applications and advanced capabilities (because of the size of the training data and the number of parameters).

As AI evolves, it is vital to ensure that diverse perspectives are included while framing the principles that govern it. Further, these principles need to be harmonised at both the state and sectoral levels. The need for state-level alignment has become a priority, and various Indian states have begun to introduce AI initiatives to improve public service delivery. For instance, Maharashtra has launched an AI chatbot that provides information on 1,400 public services;[19] Telangana uses drones for the last-mile delivery of medical supplies[20] and urban mapping;[21] and Tamil Nadu uses an AI-based app for pest control.[22] These diverse applications of AI need to follow a consistent set of norms and principles in order to ensure coherence and uniformity at the pan-India level.

At the sectoral level, there is considerable activity around the creation of sector- and model-specific guidelines. The Indian Council of Medical Research (ICMR) has released guidelines for ethical AI in the health sector,[23] and the National Association of Software and Service Companies (NASSCOM) has published guidelines for responsible generative AI.[24] These guidelines will shape AI development in the years to come, and every effort must be made to ensure that the underlying principles of these guidelines are aligned with national priorities.

The development of AI regulation and norms does not necessitate the formulation of new laws. Instead, provisions in existing laws such as the Digital Personal Data Protection Act, the Information Technology Act, and the Criminal Procedure Code could be explored with a view to close existing gaps in AI regulation.

The implementation of AI guardrails also needs to be cost effective in order to avoid limiting their application. For example, complex implementation processes can create barriers to effective data collection, especially at the grassroots level. Guardrails should be established while accounting for the operational realities of the implementing agencies, such as underfunded health centres, in order to avoid paralysing their effectiveness or pricing out smaller players from the market. This approach would facilitate the generation of more representative datasets and encourage the inclusion of a diversity of perspectives in AI innovation.

Strengthening AI Ecosystems

In order to strengthen India's AI ecosystem, it is essential to fortify its five pillars:

- **Academia:** Indian universities are the hub of innovation and a leading source of talent for tech firms. Universities need to incorporate AI into their curriculum, boost teaching and learning in the domain, and systematically encourage and incubate AI ventures while ensuring that these efforts are aligned with national goals.

- **Startups:** Startups often face challenges related to funding and technical and human capacity. Consequently, they prefer to use existing AI models rather than creating new models. Therefore, Indian startups need to be incentivised to develop homegrown AI applications.

- **Policymakers and government institutions:** There is a need to identify the policymakers and regulatory institutions that are best suited to frame laws pertaining to the governance of AI and ensure a high degree of AI literacy and awareness among them. Established precedents for appointing regulators may not be successful because of the rapidly evolving nature of the field. Instead, there is a need for multifunctional teams with an agile mindset to formulate and manage regulations.

- **Multinational corporations:** Tech multinationals and private players are the primary investors in AI in India. Therefore, they are key stakeholders in the regulatory landscape of AI in the country, and their views and perspectives should be integrated into policymaking processes.

- **Public-private partnerships (PPPs):** PPPs could be explored more closely for supporting AI governance. Collaborations between governments, the private sector, and civil society organisations (CSOs) under PPPs could help execute industry self-regulation measures, the formation of AI ethics advisory boards, and the co-design of AI policies, as well as strengthen the public-sector adoption of AI.[25] Training data collaborations will also be important for India because AI algorithms are often decision makers, and AI biases are a function of the training datasets fed into the algorithms.[26]

Another key aspect of building a strong AI ecosystem is enhancing the protection offered to upcoming developers under new regulations, particularly developers who might lack substantial financial backing. Large AI models and platforms have large teams, but historically, innovation has tended to come from small groups. Therefore, AI regulations should focus less on minor use cases and be chiefly concerned with large conglomerates that possess the size and scale to cause widespread harm.

India should take its time to frame appropriate AI laws, drawing on existing national technology policies and incorporating relevant features from international initiatives such as the OECD AI Principles,[27] the EU AI Act,[28] and the G7 Guiding Principles.[29] This would also ensure that India's AI ecosystem continues to evolve organically, without the potential stagnation caused by hard regulations. On the other hand, some experts believe that regulations around a rapidly evolving technology like AI will need constant modifications or replacement, and therefore, flexibility should be the focus of these laws. This is reminiscent of the case of mobile phones, which led to widespread conflicts between operators, policymakers, and regulators that could only be resolved once the technology reached maturity.

Conclusion and Recommendations

I ndia has a unique opportunity to craft and nurture its AI ecosystem, whether by developing novel policy approaches or adopting and adapting elements from other regulatory frameworks. While India may adopt a short-term or long-term approach, the growing use of AI across sectors is set to transform the country's digital landscape.

Based on the roundtable discussion, the following upstream (policy-level) and downstream (programmatic) actions are recommended:

- As the use of generative AI continues to grow, users and other technical and non-technical stakeholders need to be educated about its promises and perils. Awareness campaigns and drives led by the government, media, private sector, and civil society could contribute significantly in this regard.

- It is necessary to determine which parts of the AI tech stack need to be regulated and whether sectoral or risk-based approaches should be adopted. Where appropriate, AI systems should accommodate human interventions for the purpose of strengthening checks and balances rather than relying solely on automation.

- A nodal agency for licensing AI technology and service providers is recommended. All AI developers should use services from licensed providers. Adhering to established standards and possessing credentials such as certifications and accreditations could help build trust, serve as a buffer against possible harms, and provide some assurance of safe solutions.

- Given that certain existing Indian laws can address specific AI-related harms such as deepfakes and data breaches, it may not be necessary to develop new laws. Instead, the focus should be on plugging gaps in the current legal system and implementing precision regulation with a graded approach to penalties.

- Nurturing and advancing India's AI ecosystem should be one of the primary objectives of policy and programmatic efforts. Multiple stakeholders, including the government, academia, tech firms, and CSOs, will need to work together. This is also an opportune moment for India to analyse upcoming regulatory frameworks for AI across the globe and incorporate suitable elements into its own laws while ensuring that these are aligned with national interests.

- AI regulations should not be instituted at the cost of compromising or disrupting tech developers who lack significant financial backing, since they constitute a key source of innovation and are assets to the AI ecosystem.

Annex

Tech Huddle | AI Governance in India: Aspirations and Apprehensions

23 November 2023

New Delhi

Attendees

<u>Lead speakers</u>

Amoha Basrur, Observer Research Foundation

Anirban Sarma, Observer Research Foundation

Ashutosh Chadha, Microsoft

Jameela Sahiba, The Dialogue

Kumardeep Banerjee, Information Technology Industry Council

Pranjal Sharma, Economic analyst and author

<u>Discussants</u>

Aishwarya Giridhar, Centre for Communication Governance (CCG), National Law University (NLU) Delhi

Aman Taneja, Ikigai Law

Aroon Deep, The Hindu

Chetna Kumar, The Asia Group

Chhavi Sharma, Jesus and Mary College, University of Delhi

Harshit Kacholiya, iSPIRT

Ila Bose, Aumtech

Kamesh Shekar, The Dialogue

Kirti Pandey, GIZ India

Lalantika Arvind, Koan Advisory Group

Majid Durrani, Coca Cola

Mohit Chawdhry, Esya Centre

Nidhi Singh, CCG, NLU Delhi

Prateek Tripathi, Observer Research Foundation

Sachin Kumar, Cluster Innovation Centre, University of Delhi

Shankar Bose, Aumtech

Simrandeep Singh, NASSCOM

Sudhansu Nayak, CMS IT Services

Tejaswita Kharel, CCG, NLU Delhi

Endnotes

1   James Manyika and Jacques Bughin, "The Coming of AI Spring," McKinsey Global Institute, October 14, 2019, https://www.mckinsey.com/mgi/overview/in-the-news/the-coming-of-ai-spring.

2   "Top Artificial Intelligence Stats You Should Know About in 2024," Simplilearn, November 7, 2023, https://www.simplilearn.com/artificial-intelligence-stats-article.

3   Aayush Mittal, "AI Startup Investments Surge in 2023," Techopedia, November 22, 2023, https://www.techopedia.com/ai-startup-investments-surge-in-2023.

4   "Top Artificial Intelligence Stats You Should Know About in 2024"

5   Google, *Perspectives on Issues in AI Governance*, 2019, https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf.

6   G20, *G20 New Delhi Leaders' Declaration*, 2023, https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20-New-Delhi-Leaders-Declaration.pdf.

7   United Nations India, 2023,https://india.un.org/en/250912-un-secretary-general-launches-ai-advisory-body-risks-opportunities-and-international#:~:text=The%20Body%20will%20help%20bridge,place%20on%2027%20October%20 2023.

8   NITI Aayog, *National Strategy for Artificial Intelligence*, 2018, https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf.

9   Gayathri Haridas, Sonia Sohee, and Atharva Brahmecha, "The Key Policy Frameworks Governing AI in India," Access Partnership, October 2, 2023, https://accesspartnership.com/the-key-policy-frameworks-governing-ai-in-india/.

10 Shouvik Das, "IT Min to Support Development of Data for AI Models," *Mint*, October 13, 2023, https://www.livemint.com/technology/it-min-to-support-development-of-data-for-ai-models-11697217531226.html.

11 Microsoft, *Governing AI: A Blueprint for India*, 2023, https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2023/08/MSFT_Governing_AI_BlueprintFuture_India_Web.pdf.

12 Rockwell Anyoha, "The History of Artificial Intelligence," Harvard University, August 28, 2017, https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

13 David Petersson and Cameron Hashemi-Pour, "AI Vs. Machine Learning Vs. Deep Learning: Key Differences," TechTarget, November 14, 2023, https://www.techtarget.com/searchenterpriseai/tip/AI-vs-machine-learning-vs-deep-learning-Key-differences.

14 "The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023," Gov.uk, November 1, 2023, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.

15   Shaoshan Liu, "India's AI Regulation Dilemma," *The Diplomat*, October 27, 2023, https://thediplomat.com/2023/10/indias-ai-regulation-dilemma/.

16   Ministry of Electronics and IT, Government of India, 2022, https://pib.gov.in/PressReleasePage.aspx?PRID=1877739.

17   Auxane Boch, Ellen Hohma, and Rainer Trauth, "Towards an Accountability Framework for AI: Ethical and Legal Considerations," Institute for Ethics in Artificial Intelligence, February 2022, https://ieai.mcts.tum.de/wp-content/uploads/2022/03/ResearchBrief_March_Boch_Hohma_Trauth_FINAL.pdf.

18   "4 Reasons Why OpenAI Project Q* Could Be a Danger to Humanity," *India Today*, November 28, 2023, https://www.indiatoday.in/technology/news/story/4-reasons-why-openai-project-q-star-could-be-a-danger-to-humanity-2468565-2023-11-28.

19   "Government of Maharashtra Launches Aaple Sarkar Chatbot With Haptik," *The Economic Times*, March 5, 2019, https://economictimes.indiatimes.com/news/politics-and-nation/government-of-maharashtra-launches-aaple-sarkar-chatbot-with-haptik/articleshow/68268917.cms.

20   Syed Mohammed, "Telangana Launches 'Medicine from the Sky' Project to Drone-Deliver Vaccines, Medicines to Remote Areas," *The Hindu*, September 11, 2021, https://www.thehindu.com/news/national/telangana/telangana-launches-medicine-from-the-sky-project-to-drone-deliver-vaccines-medicines-to-remote-areas/article36401406.ece.

21   S. Bachan Jeet Singh, "First Time Ever, Hyderabad Municipal Corporation to Use Drones for Mapping Urban Properties," *The New Indian Express*, June 16, 2019, https://www.newindianexpress.com/cities/hyderabad/2019/jun/16/first-time-ever-hyderabad-municipal-corporation-to-use-drones-for-mapping-urban-properties-1990843.html.

22   "AGRI-Uzhavan," Government of Tamil Nadu, https://www.tnagrisnet.tn.AGRI-Uzhavangov.in/people_app/.

23   Indian Council of Medical Research, *Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare*, 2023, ttps://main.icmr.nic.in/sites/default/files/upload_documents/Ethical_Guidelines_AI_Healthcare_2023.pdf.

24   NASSCOM, *Responsible AI Guidelines for Generative AI, June 2023*, NASSCOM, 2023, https://www.nasscom.in/ai/img/GenAI-Guidelines-June2023.pdf.

25   Cas Proffitt, "Public-Private Partnerships for AI Governance: Encouraging Cooperation Between Stakeholders," Medium, June 13, 2023, https://medium.com/the-guardian-assembly/public-private-partnerships-for-ai-governance-encouraging-cooperation-between-stakeholders-ec6458a63a46.

26   Pranjal Sharma, "AI's Fuel: Why the World is Teaming Up for Datasets," *India Today*, November 26, 2023, https://www.business-standard.com/technology/tech-news/ai-s-fuel-why-the-world-is-teaming-up-for-datasets-123112600913_1.html.

27   Organisation for Economic Development and Co-operation, *OECD AI Principles*, 2019, https://oecd.ai/en/ai-principles.

28   "EU AI Act: First Regulation on Artificial Intelligence," European Parliament, June 14, 2023, https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

29   The White House, Government of the United States of America, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/.

About the Authors

Pranjal Sharma, *Economic analyst and author,* The Next New: Navigating the Fifth Industrial Revolution (HarperCollins, 2023)

Anirban Sarma, *Deputy Director, ORF Kolkata; Senior Fellow, ORF Centre for New Economic Diplomacy*

Amoha Basrur, *Research Assistant, ORF*

Prateek Tripathi, *Research Assistant, ORF*

Cover photo by Getty Images/Yuichiro Chino