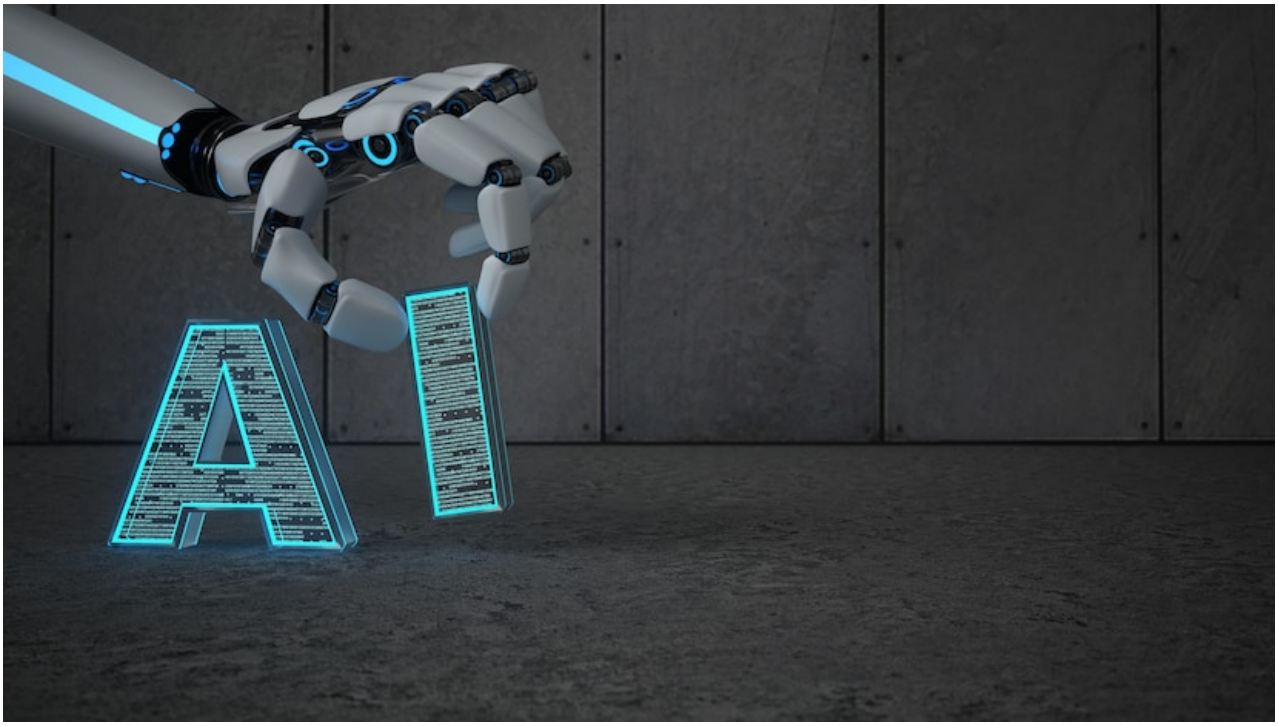
Regulation.ai@India: Striking a balance between innovation and safety

business-standard.com/opinion/columns/regulation-ai-india-striking-a-balance-between-innovation-and-safety-124091901354_1.html

September 19, 2024

India must not delay implementing comprehensive AI regulations to ensure technology serves humanity's best interests and upholds core values



(Photo: Shutterstock)

Ajay Kumar

5 min read Last Updated : Sep 19 2024 | 9:52 PM IST

The European Union led the way in data protection by introducing the General Data Protection Regulation in 2018. Now, it has again taken the lead with the AI Act, aimed at preventing potential harms from uncontrolled artificial intelligence (AI) use. India, which took nearly five additional years to implement its Digital Personal Data Protection (DPDP) Act, cannot afford a similar delay with its AI regulation.

The discussion around the need for AI regulation is increasingly relevant because AI, in the hands of malicious actors, poses significant risks to society. AI can easily compromise cybersecurity, jeopardising the entire digital landscape. It can invade privacy, enable unauthorised surveillance, facilitate cybercrime, automate attacks, and even create autonomous weapons. Moreover, AI can blur the distinction between fact and fiction through deepfakes and misinformation, manipulate public opinion, and harm mental health by encouraging addictive behaviours and distorting social dynamics.

One of the lesser-discussed but potentially most serious long-term harms of AI is its impact on human learning. In his book Trapped in the Net: The Unanticipated Consequences of Computerisation, Gene Rochlin explains that human learning benefits from the friction experienced in dealing with natural challenges we face in the real world. Automation and technology reduce these challenges, making it harder for us to solve problems and handle crises. The 2009 crash of Air France Flight 447 over the Atlantic Ocean occurred because the aircraft's fly-by-wire system encountered a storm, and the pilots, accustomed to automation, were unable to manually manoeuvre out of the storm. AI could create even more reliance on technology, further reducing our ability to solve problems and adapt to challenges.

Yet, technological advancements need to be embraced because their benefits often outweigh the risks. AI is no different; it offers great potential benefits if its risks are properly managed through regulation.

For a rapidly developing country like India, AI could play a crucial role in enhancing agricultural productivity, improving education, and advancing health care for its underserved populations. AI could be the key to accelerating India's growth and achieving its vision of Viksit Bharat. To harness AI's potential while minimising its risks, India needs to create a supportive ecosystem for its development and use. Given that a large portion of India's population has recently entered the digital world and may lack the awareness and precautionary measures found in more developed economies, careful consideration and proactive measures are essential.

India's AI regulatory framework could be built on a 3-3-3 framework. The first 3 relates to three key principles: Permissive development ecosystem, which encourages a supportive environment for the development of AI technologies; risk-based categorisation, which classifies AI applications based on their potential for harm and address them according to their risk levels; and effective accountability and liability, which, while fostering innovation, also establishes a swift and effective system for accountability and liability to manage any adverse effects.

A permissive development system should result in minimal restrictions on the development of AI for legitimate purposes. It must foster an environment where best practices and standards can be established, focusing on model development, data

quality, and skill enhancement. The IndiaAI Mission approved earlier this year is a step in this direction.

Risk-based categorisation is crucial in managing AI applications based on their potential for harm. The apps can be categorised into three risk levels: Limited, moderate and high. Before deployment, AI applications should undergo risk assessment by third-party professionals to determine their appropriate risk category. Limited risk applications, subject to minimal regulation, would involve self-certification by developers to ensure adherence to established best practices, with transparent declarations for users. Moderate risk applications would require developers and deployers to follow governance practices, ensuring adoption of ethical and transparent practices, removal of biases in data bases, and such others checks and balances required to mitigate the risks in such apps. The norms for these would be set by the regulator, which will also maintain oversight through periodic third-party audits to ensure compliance. High-risk applications, however, would undergo detailed regulatory scrutiny pre-deployment, with stringent oversight mechanisms. High-risk apps that could significantly impact human life, national sovereignty, or public order may only be deployed under government supervision and should mandatorily include human-in-the-loop — that is, the model must involve human interaction.

An accountability and liability framework for AI should clearly define the responsibilities of all stakeholders, including developers, deployers, and users. Developers should be accountable for ensuring that AI systems are free from biases, protect privacy, and undergo proper risk assessments. Deployers should be responsible for the ongoing oversight and monitoring of AI systems, including having mechanisms in place to quickly detect and mitigate any potential harm. Users should be responsible for understanding the limitations and potential consequences of the AI systems they use.

Additionally, regulators should ensure that every AI system maintains an audit trail of its decision-making processes to facilitate investigations and forensics, ensuring transparency and accountability. Provisions for compensation should be established for any harm caused.

The proposed AI regulation framework could create new roles for risk analysts to assess AI application risks, and AI forensics experts to audit and investigate AI systems. This will open up new career opportunities in AI. However, no new inspectors should be created as part of AI regulation. The government should act as a facilitator, setting rules and standards and developing skilled professionals like risk analysts and AI forensic experts. The standards will have to be sector-specific and should preferably be led by professionals and experts from relevant stakeholders.

In conclusion, India must establish an effective regulatory framework for AI to harness its potential while minimising risks. This framework should encourage innovation and growth while ensuring responsible, ethical, and transparent use of AI. The time to act is now to ensure that AI serves humanity’s best interests and upholds core values.

The writer, a former defence secretary, is distinguished visiting professor, IIT Kanpur

Also Read