"AI AND ROBOTICS IN INDIA: THE URGENT NEED FOR COMPREHENSIVE REGULATION."

Adv. Akshay P. Dhage
B.Tech, M.A., LL.B., LL.M.
Visiting Faculty at Government Law College, Mumbai.

Abstract

The rapid advancement of Artificial Intelligence (AI) and Robotics has revolutionized industries, governance, and daily life. However, the Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023, which dominate India's legal system, are unable to handle the moral, legal, and accountability issues raised by these technologies. This paper critically examines the gaps in India's regulatory landscape concerning AI and robotics, emphasizing risks such as autonomous decision-making, algorithmic bias, data privacy concerns, cyber security threats, and ethical dilemmas. The paper also analyzes India's National Strategy on Robotics1 and proposes a comprehensive regulatory framework inspired by international best practices, including the European Union's AI Act2 and the United States' AI Risk Management Framework.3 The study suggests the establishment of a centralized regulatory authority, incorporation of ethical safeguards, and adoption of a risk-based model to ensure responsible AI and robotics development while fostering innovation.

1Ministry of Electronics and Information Technology, "National Strategy on Robotics: A Vision for India." **https://www.meity.gov.in/writereaddata/files/Draft-National-Strategy-Robotics.pdf** (last visited: February 11, 2025).

2 EU AI Regulation - EU - 2024/1689 - EN-EUR-LEX., Available at: **https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32024R1689** (last visited: February 11, 2025).

3 U.S. Department of Commerce, "Artificial Intelligence Risk Management Framework:
Generative Artificial Intelligence Profile." In NIST Trustworthy and Responsible AI (NIST AI 600-1). Available at:
https://doi.org/10.6028/NIST.AI.600-1 (last visited on February 11, 2025).

KEYWORDS

AI Regulation in India, Artificial Intelligence and Robotics, Legal Framework for AI, Ethical Challenges in AI, National Strategy on Robotics, Algorithmic Bias and Accountability

Introduction

The swift progress of Artificial Intelligence (AI) and Robotics has marked the new era of technological innovation, transforming industries, economies, and societal structures. The term artificial intelligence refers to a field of study that focuses on simulating how the human brain functions in order to complete challenging tasks that people execute. 4 From healthcare and education to defense and transportation, AI and Robotics are reshaping the way we live and work. However, these advancements also bring forth complex legal, ethical, and regulatory challenges. In India, the existing legal framework, primarily governed by the Information Technology Act, 2000 (IT Act), is ill-equipped to address the unique issues posed by AI and Robotics. While the IT Act was groundbreaking at the time of its enactment, it was designed for a pre-AI era and does not account for the autonomous decision-making capabilities of modern AI systems or the integration of robotics into everyday life.

The amalgamation of AI and robotics presents a particularly potent combination, capable of both tremendous benefits and significant risks. From autonomous drones to AI-driven healthcare robots, the potential for harm, whether through algorithmic bias, data breaches, or even physical harm caused by malfunctioning robots is substantial. Yet, India lacks a dedicated regulatory framework to govern this amalgamation, leaving a dangerous vacuum in the legal landscape. 4 Yadav N. "Ethics of Artificial Intelligence and Robotics: Key Issues and Modern Ways to Solve Them."- "Journal of Digital Technologies and Law." 2023;1(4):955-972. https://doi.org/10.21202/jdtl.2023.41 (last visited on February 11, 2025).

This paper explores the limitations of the current legal framework in India, examines the risks associated with the unregulated growth of AI and robotics, and proposes a comprehensive regulatory approach to address these challenges. By drawing parallels with international frameworks and incorporating insights from other Indian legislations, this paper aims to provide a roadmap for India to navigate the complexities of AI and robotics regulation.

The Current Legal Framework: A Pre-AI Era Legislation

1. The IT Act, 2000: Outdated and Inadequate

The Information Technology Act of 2000 (IT Act) was passed in order to combat cybercrimes and provide electronic transactions a legal status. However, it was drafted at a time when AI and robotics were not mainstream concerns. As a result, the Act lacks provisions to address the unique challenges posed by AI-driven systems, such as autonomous decision-making, algorithmic bias, and the ethical implications of robotics.

For instance, Section 43A of the IT Act mandates compensation for negligence in handling sensitive personal data, but it does not address the complexities of AI-driven data processing, such as real-time data collection by autonomous systems or the use of predictive analytics.5 Similarly, Section 66 of the Act, which deals with computer related offenses, does not account for AI-specific harms like deep fake frauds or autonomous cyber attacks.6 The IT Act also fails to address the issue of algorithmic accountability. If an AI system makes a decision which results in damage or harm, then it is unclear that who should be held responsible. Is it the Developer, the Manufacturer, or the User ? This lack of clarity

5 Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), Section 43A.

6 Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), Section 66.

could lead to prolonged legal battles and undermine public trust in AI-driven technologies.

2. The Digital Personal Data Protection Act, 2023: A Step Forward, But Not Enough

The recent legislation, Digital Personal Data Protection Act, 2023 (DPDP Act) ushered a significant step towards strengthening the data protection in India. However, it falls short of addressing the specific challenges posed by AI and robotics. While the DPDP Act introduces concepts like data minimization and accountability, it does not provide a comprehensive framework for regulating AI-driven decision-making or the ethical use of robotics.

For example, the DPDP Act does not explicitly address the issue of Algorithmic Bias. In Algorithmic Bias, AI systems may inadvertently discriminate against certain groups based on biased data sets. This is a critical gap, especially in sectors like healthcare and finance, where AI-driven decisions can have far-reaching consequences.

3. Other Relevant Legislations: Gaps and Limitations

In addition to the IT Act 2000 and the DPDP Act 2023, other Indian legislations, such as the Consumer Protection Act, 2019 and the Competition Act, 2002, also play a role in regulating AI and robotics. However, these laws were not designed with AI in mind and fails to address the unique challenges posed by these technologies.

For instance, the Consumer Protection Act, 2019 provides safeguards against unfair trade practices, but it does not specifically address the risks posed by AI-driven consumer products, such as autonomous vehicles or AI-powered home assistants.9 Similarly, the Competition Act, 2002 aims to prevent monopolistic practices, but it does not account for the potential for AI-driven platforms to engage in anti-competitive behavior, such as algorithmic collusion or predatory pricing.10

The Risks of Unregulated AI and Robotics Amalgamation

1. Autonomous Decision-Making and Accountability

Amongst other challenges posed by AI and robotics, the most pressing challenge is the issue of accountability. Unlike traditional systems, AI-driven robots can operate autonomously, making decisions without human intervention. This raises critical questions: Who is responsible when an AI-driven robot causes harm? Is it the programmer, the manufacturer, or the user? The current legal framework in India does not provide clear answers to these questions, leaving a significant gap in accountability.11

For instance, in the case of an autonomous vehicle causing an accident, neither IT Act nor DPDP Act provides a mechanism to determine liability. This lack of clarity could lead to prolonged legal battles and undermine public trust in AI-driven technologies.12

2.Data Privacy and Surveillance Risks

The integration of AI and robotics also poses significant risks to data privacy. AI systems is dependent on a vast amount of personal data in order to function effectively. This also raises concerns about data misuse and surveillance. While the DPDP Act provides some safeguards, it does not address the unique privacy risks associated with

7 Digital Personal Data Protection Act, 2023, No. 30, Acts of Parliament, 2023 (India).; Cyber Law Consulting, available at: **https://www.cyberlawconsulting.com/ai_and_data_privacy_in_India.php** (last visited on Feb 15, 2025).

8 Digital Personal Data Protection Act, 2023;Rajiv Malik. "Privacy Paradox :A digital dilemma." available at: **https://law.asia/digital-personal-data-protection-act-compliance-india/** (last visited on February 11, 2025).

9 Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).

10 Competition Act, 2002, No. 12, Acts of Parliament, 2002 (India).

11 NITI Aayog, "National Strategy for Artificial Intelligence,2021" **https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf** (last visited on February 11, 2025).

12 Ana Taveira da Fonseca, Elsa Vaz de Sequeira, and Luís Barreto Xavier “Liability for AI Driven Systems “p.No. 302. Available at; **file:///C:/Users/LAB1/Downloads/Liability_for_AI_Driven_Systems.pdf** (last visited on February 11, 2025).

AI-driven robotics, such as real-time data collection by surveillance robots (one equipped with CCTV) in public spaces.13

For example, AI-powered surveillance robots could infringe on individual privacy rights by continuously monitoring and analyzing public behavior without explicit consent. This could lead to a surveillance state,

where individuals' every move is tracked and recorded, and raising serious ethical and legal concerns.14

3. Cyber security Threats

AI and robotics also introduce new cyber security threats. Adversarial attacks, where malicious actors manipulate AI systems by feeding them misleading data, are a growing concern. Similarly, autonomous robots could be hacked and used to carry out cyber attacks or physical harm. The IT Act's cyber security provisions, such as Section 70B, which designates the Indian Computer Emergency Response Team (CERT-In) for cyber security incident responses, are inadequate to address these AI-specific threats.15

For instance, an AI-driven robot in a healthcare setting could be hacked to leak sensitive patient data. The current legal framework does not provide a mechanism to prevent or respond to such incidents effectively.16

4.Ethical Concerns: Bias, Discrimination, & Transparency

13 Anamika Kundu , Digvijay S. Chaudhary " CCTVs in Public Spaces and the Data Protection Bill, 2021" available at: **https://www.rsrr.in/post/cctvs-in-public-spaces-and-the-data-protection-bill-2021** (last visited on January 11, 2025).

14 John Cater, "The Battle for Privacy in the Age of AI-Powered Surveillance: What's at Stake in 2024?" availableat: **https://www.tlciscreative.com/the-battle-for-privacy-in-the-age-of-ai-powered-surveillancewhats-at-stake-in-2024/** (last visited on January 11, 2025).

15 Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), Section 70B.

16 Gunther Eysenbach, "Security Implications of AI Chatbots in Health Care", Vol 25, Journal of Medical Internet Research, 2023,available at: **https://www.jmir.org/2023/1/e47551/** (last visited on January 25, 2025).

The data that AI systems are trained on determines their results. The AI system is likely to generate biased results if the training data is biased. This is especially troubling in fields like criminal justice, healthcare, and finance, because prejudiced AI systems may result in the unequal treatment of particular groups.17

For example, an AI system used in hiring processes might discriminate against candidates based on gender, race, or socioeconomic background if the training data reflects historical biases.18 Similarly, AI-driven predictive policing systems could disproportionately target marginalized communities, exacerbating existing social inequalities.19

The lack of algorithmic transparency further compounds these ethical concerns. Many AI systems operate as "black boxes," meaning that even its developers are not entirely aware of the reasoning behind some of their choices. This lack of transparency makes it difficult to challenge or correct biased outcomes, undermining trust in AI-driven systems.20 When this AI amalgamates or converges itself with Robot, it becomes an Intelligent self-dependent as well as independent entity capable of taking decisions as well as capable of executing the same decisions. Looking at the challenges posed by the Robotics advancements, the Ministry of Electronics and Information Technology (MeitY) came up with a Roadmap for National Strategy on Robotics.

National Strategy on Robotics: A Roadmap for India21

17 IBM Data and AI Team, "Shedding light on AI bias with real world examples", available at: **https://www.ibm.com/think/topics/shedding-light-on-ai-bias-with-real-world-example**

18 Chen, Z. "Ethics and discrimination in artificial intelligence-enabled recruitment practices."- Humanit Soc Sci Commun 10, 567

(2023).**https://doi.org/10.1057/s41599-023-02079-x** (last visited on January 25, 2025).

19 Ibrahim Raji, Damilola Bartholomew Sholademi ,Predictive Policing: The Role of AI in Crime Prevention, Volume 13 "International Journal of Computer Applications Technology and Research",–Issue

10, p.No.76 ,available at:
https://ijcat.com/archieve/volume13/issue10/ijcatr13101006.pdf

20 Majsa Storbeck, Artificial intelligence and predictive policing: risks and challenges EUCPN (2022), p.No.10. Available at:**https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf**

21 Draft National Strategy on Robotics, Ministry of Electronics and Information Technology (MeitY), July 2023, available at: **https://www.meity.gov.in/static/uploads/2024/02/Draft-National-Strategy-Robotics.pdf**

The Draft National Strategy on Robotics, published in July 2023 by the Ministry of and Information Technology (MeitY), outlines a comprehensive roadmap for India to emerge as a global leader in robotics by 2030. The strategy emphasizes the integration of robotics with artificial intelligence (AI) and other emerging technologies to drive socio-economic transformation across key sectors such as manufacturing, healthcare, agriculture, and national security. This section analyzes the key components of the strategy, its objectives, and its implications for India's regulatory and technological landscape.

1. Vision and Objectives

The National Strategy on Robotics aligns with India's AI for All and Atmanirbhar Bharat vision, aiming to make India a global hub for robotics research, development, and manufacturing while fostering innovation and entrepreneurship.

Key objectives include:

1. Establishing India as a global robotics leader by 2030, focusing on manufacturing, healthcare, agriculture, and national security.

2. Enhancing domestic value addition to reduce import dependency.

3. Driving research and innovation through targeted investments and global collaborations.

4. Expanding robotics adoption by creating new markets and applications. These objectives are essential for leveraging robotics' transformative potential while addressing technological challenges.

2. Focus Areas for Robotics Adoption

The strategy prioritizes four key sectors for robotics adoption, each with significant socio-economic impact:

1. Manufacturing: Robotics can enhance logistics, warehousing, and production automation, with companies like Flipkart and Bajaj Auto already leveraging them for efficiency.

2. Healthcare: Robotics can address workforce shortages and infrastructure gaps through surgical robots, telemedicine, and disinfection systems. According to GlobalData's report, India's market is expected to account for approximately 6% of the Asia-Pacific market in 2024, driven by government efforts to promote the adoption of surgical robotics.22

3. Agriculture: Robotics can improve productivity and safety through precision farming, crop scouting, and automated spraying, addressing labor shortages.

4. National Security: Indigenous robotics development is crucial for mine detection, surveillance, and remotely operated vehicles (ROVs), reducing dependence on imports.

3. Strategic Recommendations

The strategy adopts a four-pillar approach to strengthen India's robotics ecosystem:

1. Research and Development (R&D): Establishing Centers of Excellence (CoEs) to drive foundational and applied research,

enhance robot functionality, and develop indigenous hardware and software. Moonshot Projects aim to advance robotics through ambitious, mission-driven research.

2. Demonstration and Testing: Setting up innovation testbeds and demonstration centers to validate robotic technologies and build public trust. Regulatory sandboxes will ensure ethical and safety compliance in a controlled environment.

3. Commercialization and Supply Chain Development: Implementing fiscal incentives like PLIs, trade benefits, and ease of doing business reforms to attract investment and boost domestic manufacturing. Robotics industrial zones will enhance supply chain efficiency.

4. Adoption and Awareness: Encouraging market expansion through public procurement, financial incentives, and technology adoption plans. Capacitybuilding initiatives and awareness campaigns will educate stakeholders and address ethical concerns. 4. Challenges and Ethical Considerations While the strategy outlines a comprehensive roadmap, it also acknowledges several challenges that need to be addressed:

22 Express Healthcare. "Robotic Surgical Systems Market Size by Segments, Share, Regulatory, Reimbursement, Installed Base and Forecast to 2036,"
https://www.expresshealthcare.in/news/india-robotic-surgical-systems-market-to-record-10-percent-cagr-during-2024-36-driven-by-increasing-adoption/448103/

Skilled Workforce: The Indian robotics ecosystem faces a shortage of skilled professionals, particularly in areas like robot maintenance and integration. The strategy emphasizes the need for dedicated robotics education programs and up skilling initiatives to bridge this gap.

High Costs and Import Dependency: The high cost of robotics components and reliance on imports are significant barriers to adoption. The strategy proposes measures to localize the supply chain and reduce costs through economies of scale.

Ethical and Regulatory Concerns: The strategy highlights the need for ethical frameworks and governance mechanisms to ensure the responsible use of robotics. This includes addressing issues like algorithmic bias, data privacy, and job displacement due to automation.

The **Draft National Strategy on Robotics** aims to harness robotics and AI for socioeconomic transformation, focusing on manufacturing, healthcare, agriculture, and national security. Its success hinges on effective implementation, stakeholder collaboration, and a strong regulatory framework for ethical use.

By promoting indigenous innovation, skill development, and ethical governance, the strategy aligns with India's AI vision. To achieve global leadership, India must also address the ethical and societal impacts of robotics for sustainable and inclusive growth.

Critical Gaps in the Draft National Strategy on Robotics

Lack of Concrete Implementation Roadmap

While the strategy lays down broad recommendations, it lacks a detailed timeline for execution. The absence of phased implementation plans raises concerns about its practical applicability. The effectiveness of technology policies improves significantly when accompanied by structured roadmaps with well-defined milestones and accountability measures.

Limited Focus on Ethical and Legal Considerations

Although the strategy emphasizes technological advancements, it does not sufficiently address ethical concerns such as data privacy, job displacement, and liability in case of robot-induced harm. AI-driven automation necessitates a robust legal

framework to manage liability and ensure ethical compliance.

Absence of Financial Commitment and Incentives

The strategy does not specify financial allocations for R&D, startup support, or incentive structures for private-sector participation. Companies that effectively leverage AI-driven transformation have achieved revenue growth that surpasses their competitors by 15%. By 2026, this gap is projected to expand beyond twice its current size, reaching 37%.23

Overlooking Socioeconomic Implications

The strategy prioritizes economic benefits but does not adequately address the potential negative impacts of automation on employment, especially in labor-intensive sectors.

Weak Industry-Academia Collaboration Framework

While the document mentions fostering innovation, it lacks a concrete mechanism for industry-academia collaboration. Encouraging direct partnerships between universities & robotics firms could accelerate commercialization efforts.

Opportunities for Improvement

Integrating Legal and Ethical Safeguards

A dedicated section should address AI ethics, liability frameworks, and compliance with international robotics regulations. This would enhance public trust in robotics deployment. Developing a Detailed Implementation Plan The strategy should include a clear, time-bound roadmap with specific milestones, key performance indicators (KPIs), and responsible stakeholders for each phase of implementation. Introducing Financial Incentives and Public-Private Partnerships at:

23 Jason Angelos "Going for growth: Navigating the great value migration in the age of AI", p.No. 5, available **https://www.accenture.com/content/dam/accenture/final/accenture-com/document** 3/Accenture-Going-for-Growth.pdf#zoom=40 (last visited on February 11, 2025).

Government funding should be outlined explicitly, including tax incentives for robotics startups, grants for research institutions, and venture capital funding mechanisms to attract private investment.

Strengthening Industry-Academia Collaboration

The strategy should establish structured programs for universities to collaborate with industries on robotics development, ensuring practical exposure and innovation-driven learning. The Draft National Strategy on Robotics is a well-structured and forward-looking initiative that has the potential to position India as a global leader in robotics. However, for it to be truly effective, the strategy must include a detailed implementation roadmap, financial commitments, legal and ethical considerations, and stronger industry-academia partnerships. Addressing these gaps will ensure a more holistic and impactful adoption of robotics in India.

The Need for a Comprehensive Regulatory Framework

1.Learning from International Frameworks

India can draw valuable lessons from international frameworks like the European Union's AI Act and the United States' AI Risk Management Framework. Under the EU's AI Act, AI applications are categorized according to their risk levels, and high-risk applications-like those in healthcare and transportation-are subject to stringent controls.24

India should consider adopting a similar risk-based approach, where AI and robotics applications are classified based on their potential for harm. High-risk applications, such as autonomous vehicles and healthcare robots, should be subject to stricter

regulations, including mandatory risk assessments and ethical audits.

24 European Parliament. "Artificial Intelligence Act Proposal," COM (2021) 206 final, 2021.Avilable at: Official Journal of the European Union- https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=OJ:L_202401689#d1e3012-1-1 (last visited on February 11, 2025).

2. Establishing a Harmonized Regulatory Body

One of the key gaps in India's current legal framework is the absence of a harmonized regulatory body to oversee AI and robotics. While CERT-In25 is responsible for cyber security, it lacks the mandate to address the broader ethical and legal challenges posed by AI-driven systems. India should establish a dedicated regulatory body, similar to the European AI Board, to oversee the development and deployment of AI and robotics. This body should be tasked with developing guidelines for ethical AI deployment, conducting risk assessments, and ensuring compliance with data protection laws. It should also collaborate with international agencies to address cross-border data transfers and cyber security threats.

3. Incorporating Ethical Principles into Legislation

Incorporating ethical principles into legislation ensures fairness, accountability, and societal well-being. Laws should embed core values like justice, transparency, and human rights to address emerging challenges in technology, healthcare, and governance. A key approach is using frameworks like the European Union's AI Act, which emphasizes risk based regulation.26 Public participation and interdisciplinary input help create balanced policies that align with societal norms. Continuous legal adaptation is essential to keep pace with evolving ethical concerns. Strengthening enforcement mechanisms and ensuring accessibility to justice further enhance the effectiveness of ethical legislation. India's regulatory framework should also incorporate legislation. For instance, the ethical principles into its Right to an Explanation, as recognized under the EU's General Data Protection Regulation (GDPR), should be included in Indian law. This

25Computer Emergency Response Team- https://www.cert-in.org.in/ (last visited on February 11, 2025).

26 European Parliament. "Artificial Intelligence Act Proposal," COM (2021) 206 final, 2021. Avilable at: Official Journal of the European Union- https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=OJ:L_202401689#d1e3012-1-1 (last visited on February 11, 2025).

would ensure that individuals have the right to understand how AI-driven decisions affecting them are made.27 Additionally, the framework should mandate algorithmic transparency, requiring AI developers to disclose how their algorithms work and how they mitigate bias. This would help build public trust in AI-driven systems and ensure that they are used ethically.28 Understanding AI's impact goes beyond merely revealing the algorithm's terms. It also involves disclosing various aspects of the training data, such as its origin, extent, quality, and internal patterns. Additionally, it requires recognizing the validation methods used and, most importantly, acknowledging that complex systems often display unexpected behaviors in real-world applications. Future AI regulations must consider these multiple facets of transparency.29

4. Addressing the Risks of AI and Robotics Amalgamation

Given the unique risks posed by the integration of AI and robotics, India's regulatory framework should include specific provisions to address these challenges. For instance, the framework should mandate safety certifications for AI-driven robots, particularly

those used in high-risk sectors like healthcare and transportation.

The amalgamation of AI and Robotics presents risks such as job displacement, ethical concerns, security threats, and liability issues. Autonomous decision-making raises accountability questions, especially in high-stakes industries like healthcare and defense. 30 AI biases can lead to discriminatory outcomes, while cybersecurity vulnerabilities may result in data breaches or robotic malfunctions. Regulatory

27 General Data Protection Regulation (GDPR), Art. 22, European Union, 2018., available at: https://gdpr info.eu/art-22-gdpr/

28 Yoo, Christopher S., "Beyond Algorithmic Disclosure For AI" (2024). Articles. 426.**https://scholarship.law.upenn.edu/faculty_articles/426**

29 Ibid at 17

30 Osasona, Amoo, et.al., Reviewing The Ethical Implications Of AI In Decision Making Processes, p.No.322-335, International Journal of Management & Entrepreneurship Research P-ISSN: Volume 6, Issue 2,February 2024, Available at: **https://www.researchgate.net/publication/378295986_REVIEWING_THE_ETHICAL_IMPLICATIONS_OF_AI_IN_DECISION_MAKING_PROCESSES**

frameworks are still evolving to mitigate these risks. Implementing robust AI ethics, transparent algorithms, and legal safeguards is essential to balance innovation with safety. Continuous oversight and public discourse can help address unforeseen challenges. Additionally, the framework should establish liability rules for harm caused by autonomous robots. These rules should clearly define who is responsible, whether it is the developer, the manufacturer, or the user, and provide mechanisms for victims to seek redress.

Conclusion

India stands at the cusp of an AI and Robotics revolution, set to transform industries,
governance, and daily life. However, existing laws like the IT Act, 2000, and DPDP Act, 2023, lack the provisions to address ethical, legal, and accountability concerns of autonomous systems. Without regulatory intervention, risks such as privacy violations, biased decision-making, and cyber security threats may arise.
To ensure responsible AI adoption, India must:

1. Establish a dedicated AI and robotics regulatory body to oversee governance, assess risks, and prevent legal uncertainty.

2. Embed ethical safeguards into legislation, ensuring transparency, fairness, and accountability, with frameworks like the EU's right to explanation.

3. Adopt a risk-based regulatory model, classifying AI applications based on harm potential, with strict compliance for high-risk uses.

Proactive regulation will prevent fragmented governance, legal ambiguities, and loss of public trust. By balancing innovation with ethical responsibility, India can lead in AI and robotics while safeguarding citizens' rights.

***