THE DIGITAL INDIA ACT AND AI GOVERNANCE IN INDIA

Sapna Kumari*

INTRODUCTION

The last few years have seen a fundamental and historic change in India's digital ecosystem, an event often described as the "Digital Transformation of India." It is an evolution that goes beyond policy jargon; it marks a complete shift in the way businesses operate, how governance is delivered, how education and healthcare are made available, and how financial transactions are carried out. Government policy programs, in particular the flagship "Digital India" initiative in 2015, provided a strong policy framework and a definite action plan for this revolutionary change. The central mandate of Digital India is to bring all citizens into the digital fold, enhance their capabilities using technology, and create a "digitally empowered society and knowledge economy"

This policy initiative, alongside a growing penetration of smartphones, decreasing data prices, the increasing use of digital payment systems like the Unified Payments Interface (UPI) — which today handles billions of transactions every month — and the growth of e-governance platforms, has integrated technology into virtually every facet of Indian life. Today, nearly half a billion people own smartphones, more than 700 million are online, and digital payment platforms enable huge numbers of transactions every month. This huge digitisation has opened the door to major innovations, above all Artificial Intelligence (AI), which is best suited to take advantage of these large volumes of data to solve advanced problems economically, reliably, and at scale.

AI's built-in ability to learn from information and make decisions independently, using methodologies like machine learning, deep neural networks, and natural language processing, makes it a powerful tool to drive development across many industries. Its uses range from healthcare, where it assists in the diagnosis and tailoring of medicine; education, through

*BBA LLB, FIFTH YEAR, BABU BANARASI DAS UNIVERSITY, LUCKNOW.

adaptive and customised learning platforms; agriculture, with yield prediction and advisory; and even policing, to facilitate predictive policing, monitoring, and fraud detection.

OVERVIEW OF THE DIGITAL INDIA ACT (DIA) – PURPOSE, SCOPE, AND KEY OBJECTIVES

First brought into law in 2000, India's Information Technology Act was intended to establish a legal framework for electronic messages and transactions in an emergent digital age. It quickly became insufficient, though, as technologies that were unimaginable at the time of its creation began advancing and spreading rapidly, such as smartphones, social media, and advanced algorithmic services.[12]

To counteract these developments, the Digital India Act (DIA) has been proposed to replace and replace the Information Technology Act, 2000. The DIA seeks to update India's legal framework, making it more responsive, visionary, and holistic in its response to the complex legal and policy challenges brought by the digital revolution and the advent of Artificial Intelligence.[3]

The main aims of the Digital India Act are-

Future-Proof Infrastructure: Creating a legislative infrastructure that can accommodate emerging future technologies and trends, instead of providing solutions to existing problems.

Increased Protection: Providing efficient mechanisms to protect basic rights, including the right to privacy, freedom of expression, and equality, in the age of growing algorithmic power.

Enhancing Supervision: Developing dedicated regulatory or supervision entities to oversee digital platforms, service providers, and algorithm developers.

Accountability of Companies: Placing obligations on businesses and organisations to develop and implement their algorithms openly and ethically, with sanctions for failure to comply.

[1] https://www.delhilawacademy.com/digital-india-act/
[2] https://www.upguard.com/blog/digital-india-act
[3] https://www.delhilawacademy.com/digital-india-act/

Innovation and Regulation Balance: Establishing a framework that promotes innovation and economic development without excessively reducing potential harms, thus passing through the precarious balance pursued by policymakers.

THE INTERSECTION OF AI AND DIGITAL REGULATION: WHY THE DIA IS CENTRAL TO AI REGULATION IN INDIA

The Digital India Act arises at a pivotal moment when drastic and ubiquitous technological transformation sharply cuts against the pace of policy and legal institutional development. In this context, the Digital India Act becomes a landmark piece of legislation for regulating and guiding the future path of Artificial Intelligence in India.

AI technologies, by their nature, pose difficult questions that cut across both conventional sectoral and legal divides. For example, questions of responsibility are raised concerning who should be held accountable if an automated algorithm discriminatorily turns down a mortgage application, rejects a health benefit, or unfairly profiles a person. Transparency takes centre stage, with questions regarding the level to which corporations need to disclose their algorithms' choices—a term referred to as "algorithmic explainability"—both to regulators and consumers. In addition, the legislation needs to determine how to ban and punish algorithmic discrimination on the grounds of race, caste, gender, religion, or geography, all while at the same time upholding the right to innovate. Data protection is a second-key priority, as the effectiveness of AI depends on massive amounts of data, frequently personal and confidential, and gives rise to concerns regarding consent, ownership, storage, and cross-border transfer. Lastly, the growing dependence on automated systems raises their robustness and integrity to a national security issue, where they need stringent protection from cyberattacks and malicious tampering.

Another level of sophistication is that most companies that are building and implementing AI technologies in India are multinational corporations with headquarters outside the country. This adds to the challenge of oversight and enforcement. The Digital India Act, therefore, has to create means to exercise India's legal authority and policy interests, converge with international standards, and at the same time address the peculiar domestic realities and national priorities of the nation.

RESEARCH QUESTIONS AND METHODOLOGY

This research article strives to critically analyse the Digital India Act's regulatory approach to Artificial Intelligence and its ability to effectively mould the future of technology in India. To spearhead this research, the following research questions have been created-

1. In what way does the Digital India Act seek to regulate Artificial Intelligence technologies as part of its legal scheme?
2. To what extent is the Digital India Act aligning itself with international best practices and standards for ethical and responsible Artificial Intelligence regulation (e.g., the EU's Artificial Intelligence Act or the USA's Algorithmic Accountability Act)?
3. How does the Digital India Act address conflict resolution, consumer protection, fairness, transparency, and accountability in algorithmic decision-making?
4. What are the potential gaps, weaknesses, or deficits in the Digital India Act's policy towards Artificial Intelligence, and how can these be addressed through policy and legal reforms?

To answer the above-referred research questions, this paper adopts a normative and analytical legal approach, which include-

Doctrinal legal research: A detailed analysis of the Digital India Act text, policy documents, legislative reports, and related legal documents. This doctrinal research is concerned with the literal meaning of the provisions of the Act and their legal consequences.

Comparative analysis: The study compares India's policy framework with global regimes and best practices, namely the EU Artificial Intelligence Act and the USA Algorithmic Accountability Act. The comparison is undertaken to see areas of convergence and divergence, **and where India's approach is stronger or weaker.**

Secondary sources: The research is based on scholarly journals, policy studies, expert opinion, and empirical research to shed light on important issues, interpret legal instruments, and determine areas of policy voids.

This multi-source approach makes it possible to gain a wider picture, moving beyond the black-letter law to its possible application and future consequences.

UNDERSTANDING THE DIGITAL INDIA ACT (DIA): A FOUNDATIONAL ANALYSIS

The Digital India Act (DIA) is a resolute policy change in India's drive to govern its fast-growing digital environment. It attempts to create a forward-looking legal framework that can keep up with the radical technological revolution in communication, trade, and government. The DIA is able to switch over from the inappropriateness of the Information Technology Act of 2000 (IT Act), in its time-class-leading format, having been outpaced by smartphones, social media, Artificial Intelligence, Internet of Things, and large online websites. The IT Act was conceived for a fairly simple internet landscape and did not envision numerous modern policy issues, from harmful content and fake news to the power to shape public discourse on the part of large platforms and the need for strong oversight powers and protections of users' rights.[45]

Material gaps in the IT Act that made this legislative amendment unavoidable are the absence of distinct intermediary liabilities, weak regulatory processes, and a lack of adequate protection for digital dignity, freedom of speech, and data control. Additionally, the growing cyber threats and cases of forgery called for meaningful incident response and non-conformance penalties using a more sophisticated model. The Digital India Act attempts to remedy these lacunae by establishing definite guidelines for platform obligations, strengthening oversight mechanisms, protecting the rights of users, and countering cybersecurity risks in a coordinated and visionary approach.

The Digital India Act is organised on four pillars, all of which together constitute a strong legal framework for the digital space. The first pillar lays down a legal framework for online intermediaries that include social media platforms, messaging apps, search engines, content delivery networks, and online marketplaces. The Act requires a tiered approach, distinguishing large social media intermediaries from smaller traditional service providers, and imposes on them obligations based on their size and reach. The Act stresses responsible platform behaviour, mandating them to set up complaints mechanisms, designate a Grievance Officer, address lawful notices promptly, and comply with codes of practice. The Act further seeks to increase the accountability of platforms for the content shared through their services. The second pillar is related to user responsibilities and rights in the online environment.

[4] https://www.delhilawacademy.com/digital-india-act/
[5] https://www.upguard.com/blog/digital-india-act

The Digital India Act imposes a Digital Bill of Rights to empower citizens online. All users are qualified to enjoy equal and non-discriminatory access to online services and have their rights to respect and protection against online harassment, campaigns of disinformation, and unwarranted content bans or deletions. Significantly, the Act also embodies responsibilities in addition to these rights, compelling users to avoid spreading misinformation, cyberbullying, or restricted content, and to maintain reasonable platform norms. This balanced approach acknowledges that a successful digital ecosystem is predicated on accountable behaviour from all users. The third pillar focuses on digital safety and trust. The Digital India Act also seeks to create a more trusted digital ecosystem by countering rising cyber threats and objectionable content.

Certain kinds of content—like child pornography, terrorist communication, fraudulence, and phishing—are categorically outlawed, and they are obligated to take instant action on removal requests from the regulator or an agency with specialised expertise. Major platforms can be asked to employ automated technologies like hash-databases or content-filters to detect and filter offending content automatically. Platforms also need to make public regular reports giving details about complaints received, actions undertaken, and redressal timeframes.

For the promotion of responsible behaviour throughout the ecosystem, the Digital India Act contemplates codes of practice and ethics, which will operate as industry benchmarks for equitable and conscientious content management. The fourth pillar is concerned with data governance and cross-border implications, though this sphere is mostly governed by the Digital Personal Data Protection (DPDP) Act of 2023. However, the Digital India Act emphasises the need for protection when data crosses borders and points towards the responsibility of regulators to lay down rules for the movement of sensitive or strategic data and, in some cases, promotes data localisation to protect the information of Indian citizens.[67]

To successfully pursue these policy goals, the Digital India Act creates new institutional frameworks, namely the Digital India Authority (DIA), Digital Grievance Appellate Boards, and a Digital Advisory Council. The Digital India Authority, a standalone specialist authority, is vested with powers to oversee and govern the digital space, promulgate codes of practice, handle complaints, and impose penalties for non-compliance. The Digital Grievance Appellate Boards provide a specialised, fair, and accessible forum for appealing a platform's decision-

[6] https://www.upguard.com/blog/digital-india-act
[7] https://www.policycircle.org/opinion/big-tech-ai-regulation/

making. Furthermore, a Digital Advisory Council, which includes industry representatives, civil society organisations, academia, and government, is responsible for guiding regulators and lawmakers with regard to policy changes and future legislation.[8][9][10]

To give effect to its provisions, the Digital India Act confers enormous power on regulators. It empowers them to inflict monetary penalties and revenue-balanced penalties for default. Regulators can suspend services in the event of recurring contraventions, order the takedown of illicit content, suspend particular accounts, or temporarily disconnect services if and when required. Additionally, regulators can enforce criminal penalties on flagrant or intentional violations, fraud, or behaviour that threatens public order and children's safety.

The Digital India Act is a forward-thinking legislative model crafted to deal with the seismic changes in the 21st-century digital paradigm. It attempts to strike a fine balance: protecting users' rights, improving regulation of powerful platforms, and making available an open, secure, and innovative digital environment to everyone. By its shift from the Information Technology Act 2000 to the Digital India Act 2025, India indicates its preparedness to address the distinctive policy issues arising out of a fast-changing digital society—from fake news and cybercrime to data governance and duties of intermediaries—while maintaining its constitutional values of equality, dignity, and freedom of expression.

REGULATION OF HUMANOID AI IN INDIA: PRECEDING STRATEGIES AND POLICY DOCUMENTS

Niti Aayog's Role: The NITI Aayog (National Institution for Transforming India), India's central government think-tank, was key in driving the agenda for Artificial Intelligence (AI) governance in India. Realising the transformative ability of AI, NITI Aayog released a foundational policy document called the "National Strategy for Artificial Intelligence," popularly referred to through its hashtag AIforAll. This approach envisioned making India a leader in the global ecosystem for AI and ensuring that the advantages of AI percolate among the maximum possible sections of society. Five sectors were identified as having the greatest AI-based growth potential and were the focus of the strategy specifically: health, agriculture, education, smart mobility, and smart cities.

[8] https://www.techpolicy.press/transparency-must-be-a-cornerstone-of-the-digital-india-act/
[9] https://www.shankariasparliament.com/current-affairs/digital-india-act-2023
[10] https://informatics.nic.in/news/1455

Apart from sectoral implementation, the approach also emphasised the need for responsible AI development. As a sequel, NITI Aayog introduced a framework called "Principles for Responsible AI," which enshrined important ethical principles like trust, safety, accountability, and fairness. These principles were meant to make sure that the use of AI systems in India respected constitutional values, fundamental rights, and the public good. Trust, here, refers to the explainability and transparency of AI systems, whereas safety makes sure that AI applications are secure, reliable, and resilient. Accountability stresses the need for mechanisms to hold the users and creators of AI systems accountable for their influence, and equity encourages inclusive and non-discriminatory use of AI.

Together, NITI Aayog's work furnished the conceptual and moral bases for India's AI ecosystem, though in the guise of recommendations and policy proposals as opposed to legally enforceable provisions. This testified to the following need for a piece of legislation, i.e., the Digital India Act, to implement these maxims into enforceable provisions.

Ministry of Electronics and Information Technology (MeitY) Initiatives: AI Governance Guidelines Report (If Prepared By 2025)

The Ministry of Electronics and Information Technology (MeitY) has led the charge in dealing with the regulatory and ethical concerns of Artificial Intelligence. Its greatest achievement has been the AI Governance Guidelines Report, which, if finalised during 2025, will create a systematic and enforceable framework for the use of responsible AI in India. These guidelines are anticipated to migrate from voluntary norms to normative expectations or quasi-regulations that would be enforceable on both public and private AI developers.[11][12][13]

The report is also expected to give utmost importance to sectors like the risk categorisation of AI systems, data protection and security, transparency of algorithms, and decision-making oversight. In addition to these, the report might suggest regulatory sandboxes for testing AI applications on a pilot basis and outline an institutional framework for monitoring AI deployment in sensitive sectors. When put into practice, these rules would be a compromise

[11] https://www.obhanandassociates.com/blog/legal-perspectives-on-ai-governance-in-india-a-summary-of-the-ai-governance-guidelines-report/
[12] https://securiti.ai/ai-governance-in-india-meity-2025-report/
[13] https://www.azbpartners.com/bank/update-on-meitys-report-on-ai-governance-guidelines-development/

between soft law and legislation under the Digital India Act and comply with India's constitutional principles and global best practices in regulating AI.[14]

India AI Mission and Objectives

MeitY has initiated the IndiaAI Mission in a strategic development and operational shift as India's flag bearer program to pilot AI research, innovation, and adoption at scale. The mission will consolidate the core ecosystem for AI growth and make India a competitive force in world AI innovation. One of the main pillars of the mission is the creation of robust computing infrastructure, such as High-Performance Computing (HPC) capability and AI supercomputers, to enable start-ups, researchers, and governmental efforts.[15][16][17][18]

The other key goal is to drive the development of local AI models and datasets to decrease dependence on external platforms and build trust in locally developed systems. The mission also centres on the usage of AI in socially relevant areas like healthcare, agriculture, governance, and language processing, such as for low-resource Indian languages. Also, the mission aims to develop AI capabilities through academic collaborations, fellowships, and industry-academia collaborations. It is complemented with incentives for AI start-ups, regulatory initiatives, and undertakings to increase inclusivity and accessibility in AI implementation.

India AI Mission Key Points:

- National flagship program to increase AI infrastructure and innovation.

Predominant constituents are:

- Compute Infrastructure – Developing AI supercomputers and high-performance computing. Datasets and Platforms – Developing local, open, and reliable AI training data.

AI Applications – Promoting AI deployment in public good areas, like:

[14] https://thelondonstory.org/2025/04/15/indias-ai-governance-guidelines-report-faqs-answered/
[15] https://securiti.ai/ai-governance-in-india-meity-2025-report/
[16] https://www.obhanandassociates.com/blog/legal-perspectives-on-ai-governance-in-india-a-summary-of-the-ai-governance-guidelines-report/
[17] https://www.thebridgechronicle.com/tech/india-ai-regulation-global-model-2025
[18] https://law.asia/india-ai-regulation-focus-unified-approach/

- Healthcare (e.g., disease prediction, telemedicine).
- Agriculture (e.g., crop monitoring).
- Education (e.g., personalised learning).
- Natural Language Processing (particularly for Indian languages).

Talent and Research Ecosystem: Creating centres of excellence, AI skilling initiatives, and fellowships.

Start-up Enablement: Offering entrepreneur grants, mentorship, and regulatory facilitation to AI start-ups.

Integration of Policy and Ethics: Ensuring that the development of AI is according to constitutional and democratic values.

Sectoral Regulations with AI Dimensions (E.G., RBI for Fintech, Sebi for Capital Markets)

Before the advent of a harmonized legislation like the Digital India Act (DIA), India's approach to Artificial Intelligence (AI) regulation was, in effect, sectoral and decentralized, working within the requirements of several overseeing organizations. This implied that in the absence of an overarching AI law, many regulators indirectly touched on issues related to AI by their current legal mandate, mainly in high-risk and technology-intensive areas such as finance, healthcare, insurance, and capital markets. Of these, the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) were especially notable.

Reserve Bank of India (RBI) – Fintech and Digital Banking

The RBI, which is the central banking body of India, has led the charge in regulating AI and Machine Learning (ML) technologies in financial services, particularly in FinTech, digital lending, and banking operations. While the RBI has not made AI-specific regulations, it has made several substantive steps to address the risk generated by automated systems.

For instance, the RBI’s 2022 guidelines on digital lending included provisions addressing algorithmic decision-making, data privacy, and automated credit scoring systems. These guidelines require regulated entities to ensure human oversight and explain the ability of credit decisions, particularly when AI tools are used to assess borrower eligibility. Moreover, financial institutions that use AI for fraud monitoring, risk assessment, or customer profiling

need to provide fairness, data protection, and bias reduction under overarching RBI mandates on governance, cybersecurity, and data localisation.

The RBI has also placed a priority on consumer protection, requiring that customers must not be exposed to opaque decisions made by "black-boxed" algorithms and that the mechanism of redressal of grievances has to be strong and accessible, irrespective of the underlying layer of technology.

SECURITIES AND EXCHANGE BOARD OF INDIA (SEBI) – CAPITAL MARKETS AND ALGORITHMIC TRADING

The SEBI, the capital market regulator of India, has itself participated actively in the development of AI and algorithmic trading systems in stock exchanges and investment platforms. SEBI has put in place strict guidelines on automated and high-frequency trading (HFT) through circulars and compliance directions that indirectly govern AI-based trading systems.

The guidelines are intended to curb market manipulation, achieve systemic stability, and ensure transparency. For instance, AI or ML-based predictive trading brokers have to go through code audits, record detailed trading algorithms, and ensure that these models do not breach the norms of fair market behaviour. In some other cases, regulatory sandbox models have been offered to enable pilot testing of new AI solutions within a controlled, low-risk setting.

SEBI’s approach focuses on striking a balance between innovation and investor protection. As more wealth management platforms and robo-advisors adopt AI for client servicing and portfolio construction, SEBI’s regulatory stance ensures that these tools remain explainable, auditable, and compliant with fiduciary duties.

OTHER SECTORAL BODIES

Though RBI and SEBI are the leading regulators with AI consequences, sectoral authorities are increasingly reacting to AI adoption as well-

Insurance Regulatory and Development Authority of India (IRDAI): Examining frameworks for regulating AI usage in underwriting, claims settlement, and detection of fraud.

Telecom Regulatory Authority of India (TRAI): Tackling AI-based spam filtering and network optimisation in telecom operations.

Central Drugs Standard Control Organisation (CDSCO): Facing emerging issues with AI-facilitated medical devices and diagnostics, albeit official regulation remains in the making.

Gaps in Pre-DIA AI Governance: Why A Comprehensive Law Is Needed: Before the passage of the Digital India Act (DIA), India's AI regulation was marked by a sectoral, dispersed, and mostly non-binding system. Even though agencies such as NITI Aayog, MeitY, and sectoral regulators (RBI, SEBI, IRDAI) promulgated major guidelines and frameworks, these were not backed by the compulsive authority of law, consistency, and overall effectiveness. The cross-industry use and complexity of Artificial Intelligence created an imperative for a holistic legal framework. Some major gaps in the pre-DIA regime emphasised this necessity:[19][20][21][22][23]

Absence of a Binding Legal Framework for AI: Most of the policy reports released by MeitY and NITI Aayog were advisory; they enunciated ethical principles and best practices, but were not backed by legislation. There were no rules that could be enforced to oversee the development, deployment, or regulation of AI in India. As such, companies and developers were not legally bound to respect ethical norms like fairness, transparency, or accountability unless specially prescribed by some sectoral legislations. This context resulted in the presence of ethical intentions, but without an operationalisation that was compulsory, leaving a wide gap in ensuring ethical AI development.[24]

Horizontal Regulation Deficit between Sectors: AI technologies are ubiquitous and not limited to one industry; their uses cut across finance, healthcare, governance, education, and law enforcement. India's pre-DIA regulatory landscape was segmented, thus creating different standards in different industries. Fragmentation caused inconsistency and uncertainty in regulation. For instance, AI applied to credit scoring may be open to scrutiny by the RBI, but

[19] https://aakashi.hashnode.dev/ai-regulation-in-india-vs-the-world-are-we-ready-or-already-behind
[20] https://lawfullegal.in/the-rise-of-artificial-intelligence-and-the-legal-challenges-of-algorithmic-accountability-in-india/
[21] https://thelondonstory.org/2025/04/15/indias-ai-governance-guidelines-report-faqs-answered/
[22] https://singhania.in/blog/ai-and-indian-law-addressing-privacy-ethics-and-copyright-challenges-in-the-digital-age/
[23] https://olawebcdn.com/ola-institute/Indias_Digital_Future_Strengthening_DPDP_Rules_for_Privacy_Innovation_and_Global_Leadership.pdf
[24] https://www.techpolicy.press/transparency-must-be-a-cornerstone-of-the-digital-india-act/

counterpart systems that are used for public welfare targeting or face recognition may not be under any comparable regime, leading to regulatory blind spots for cross-cutting AI effects.

Absence of Protection of Fundamental Rights: AI systems, especially those used in public services or law enforcement agencies, have deep implications for constitutional rights such as the right to privacy, non-discrimination, and due process. Before the DIA, there were no regulations that dealt with algorithmic bias, automated decision-making, or the absence of transparency in AI systems, directly affecting citizens' rights. This became an even bigger issue after the landmark.[25]

Pettaway judgment (2017), which enshrined privacy as a fundamental right and specifically suggested that technologies such as AI should be regulated to protect human agency. Lacking an overarching framework, the capacity for AI to reinforce or further aggravate existing social disparities remained generally untamed.

No Institutional Oversight Mechanism: One major weakness was the lack of a specialised body or regulatory agency specifically responsible for monitoring, auditing, or investigating AI systems in India. Unlike the EU's AI Act, which requires a single regulator and conformity assessment protocols, India's earlier strategy lacked institutional coherence. Without an explicit oversight mandate, the power to effectively regulate risky or immoral AI deployments and to enforce compliance with developing ethical standards was greatly impaired. This absence of a single enforcement agency and specified adjudicatory mechanism left a void in accountability for AI-caused harms.[26][27][28]

CONCEPTUAL FRAMEWORK

The section here explores in greater depth the theory-based concepts that underpin the report, broadening out from the definitions and implications set out in the background, offering a solid analytical framework for the following analysis of the Digital India Act.

Digital Transformation in India: Beyond Policy Catchphrases: The "Digital Transformation of India" is not only a policy drive but a deep social transformation affecting

[25] https://lawfullegal.in/the-rise-of-artificial-intelligence-and-the-legal-challenges-of-algorithmic-accountability-in-india/
[26] https://www.techpolicy.press/indias-ai-governance-guidelines-report-a-medley-of-approaches/
[27] https://aakashi.hashnode.dev/ai-regulation-in-india-vs-the-world-are-we-ready-or-already-behind
[28] https://thelondonstory.org/2025/04/15/indias-ai-governance-guidelines-report-faqs-answered/

all aspects of life, ranging from enterprise and administration to learning, medicine, and finance. This ubiquitous transformation has provided fertile ground for enormous innovations, especially in Artificial Intelligence, which can harness humongous data volumes to address intricate challenges inexpensively and on a large scale. This change is underpinned by a strong policy framework, which the "Digital India" initiative of 2015 is an example of, with its objective of taking citizens online, equipping them with technology, and creating a "digitally empowered society and knowledge economy". This aspiration has been driven by a tremendous rise in smartphone penetration, with almost half a billion citizens possessing smartphones currently, along with declining data prices, the mass popularity of digital payment systems such as UPI (handling billions of transactions every month), and the growth of e-governance platforms.

The mass scale and velocity of India's digital uptake, as well as its socio-economically diverse demographics, make for a singular and complicated regulatory context. The mass and rapid digital reach, which is attested by hundreds of millions of internet users and billions of monthly digital transactions, inevitably poses huge opportunities for economic development and social well-being. But such speedy growth also brings huge risks around data privacy, algorithmic bias, and digital exclusion if not suitably controlled. Such magnitude means that any regulatory approach, even the DIA, needs to be extremely flexible, scalable, and inclusive. A well-functioning regulatory system in India, considering its context—that is, multiple languages, different digital literacy, and existing social disparities—would be a very useful model to be followed by other developing countries with similar kinds of problems. This would be a better option than the mere imitation of models of digitally advanced Western countries. At the same time, any regulatory failure could have far-reaching and devastating negative consequences for a huge population.

Artificial Intelligence: Capabilities and Governance Implications: The fundamental strength of AI is its capacity for learning from data and autonomous decision-making without specific human direction, based on methods like machine learning, deep neural networks, and natural language processing. This transforms AI into a revolutionary device in various fields, such as healthcare (diagnostics, personalised medicine), education (adaptive learning), agriculture (yield forecasting), and law enforcement (predictive policing, fraud detection). India's strategic AI vision, as encapsulated in NITI Aayog's "National Strategy for Artificial Intelligence" (#AIforAll), seeks to position India at the cutting edge of the world AI ecosystem

to ensure that AI benefits reach the widest possible societal reach, especially across five high-priority sectors: health, agriculture, education, smart mobility, and smart cities. In addition to this, NITI Aayog also suggested "Principles for Responsible AI", emphasising trust, safety, accountability, and fairness, aimed at harmonising AI applications with constitutional values and basic rights.

MeitY's "AI Governance Guidelines Report" (anticipated 2025) will also seek to provide a systematic and enforceable framework for responsible AI, possibly on risk classification, data protection, algorithmic explainability, and monitoring. The "IndiaAI Mission" is a flagship program for accelerating AI research, innovation, and use, with a focus on compute infrastructure, local AI models/datasets, applications in public interest, talent growth, and start-up facilitation, while mainstreaming policy and ethics.[29][30][31][32]

The twin focus on "AI for All" (encouraging broad adoption for the good of society) and "Safe & Trusted AI" (reducing harm) imposes a basic tension on India's AI policy, requiring a very fine-grained regulatory method. The direct emphasis by efforts such as NITI Aayog's #AIforAll and MeitY's IndiaAI Mission on utilising AI for "inclusive growth and social well-being" and use in "socially relevant areas" reflects a national intention of inclusive societal good. At the same time, the MeitY guidelines and the expressed purpose of the DIA convey the imperative need for "Safe & Trusted AI".

This presents a policy challenge: fast and mass deployment of AI in core public domains, like healthcare, education, or social welfare allocation, to "AI for All" objectives might unintentionally enhance the effect of defective, biased, or uncontrolled AI systems on vulnerable groups. The risk is especially high in a nation that already has socio-economic inequalities, where algorithmic bias may augment disparities. Thus, the "Safe & Trusted AI" pillar is not just an ethical one but a fundamental protection from unwanted negative societal interactions and public loss of trust, to facilitate long-term adoption of AI. This means that the DIA should not just establish general moral guidelines but also require intense, context-based risk assessments and safeguards for AI use in public-facing and high-impact sectors, possibly

[29] https://www.obhanandassociates.com/blog/legal-perspectives-on-ai-governance-in-india-a-summary-of-the-ai-governance-guidelines-report/
[30] https://securiti.ai/ai-governance-in-india-meity-2025-report/
[31] https://thelondonstory.org/2025/04/15/indias-ai-governance-guidelines-report-faqs-answered/
[32] https://www.azbpartners.com/bank/update-on-meitys-report-on-ai-governance-guidelines-development/

requiring even greater oversight for AI systems deployed in government services or by large platforms.[33]

Algorithmic Accountability: Definition, Components, and Significance: Algorithmic accountability is a central legal issue raised by AI systems, meaning responsibility for decision outcomes taken by algorithms. Transparency is the fundamental element of algorithmic accountability, which means knowing how the AI works, making it explainable, and let users know when they are communicating with an AI system. Fairness is another essential element that is intended to avoid bias and discrimination. Auditability calls for ongoing monitoring and auditing of AI systems, while human oversight ensures that human judgment and intervention take precedence. Critical questions surround who is responsible if a computer-driven algorithm inflicts harm, e.g., discriminatory denial of a mortgage loan application, the level of explainability required by an algorithm, and how to avoid discrimination while promoting innovation. Before the DIA, Indian law, especially in the realm of torts and contracts, was not clear on the responsibility of AI developers, operators, or users in case of injury.[34][35][36][37]

The quest for "algorithmic accountability" in India is especially difficult in light of the sudden digitisation of a diverse population base and the dominance of multinational AI creators, who require strong extraterritorial jurisdiction and technical enforcement capacity. The question of who is liable if an automated algorithm does harm, i.e., discriminatorily rejects a mortgage application or profiles the person, is complicated by the reality that many AI companies that are operating in India are headquartered elsewhere. That is, they are multinational corporations based elsewhere. This is a problem of enforcement. The success of DIA in enshrining genuine algorithmic accountability would also depend on not just specifying well-defined liability frameworks in India but also on its powers to invoke extraterritorial jurisdiction and force compliance upon foreign entities. This could involve making provisions for data localisation or robust cross-border data transfer protocols. In addition, holding accountable sophisticated, proprietary "black-box" algorithms created by international technology giants will necessitate the Digital India Authority to be exceptionally technologically skilled and investigative. The power to request and understand "algorithmic explainability" will be key, suggesting a

[33] https://lawfullegal.in/the-rise-of-artificial-intelligence-and-the-legal-challenges-of-algorithmic-accountability-in-india/
[34] https://www.obhanandassociates.com/blog/legal-perspectives-on-ai-governance-in-india-a-summary-of-the-ai-governance-guidelines-report/
[35] https://securiti.ai/ai-governance-in-india-meity-2025-report/
[36] https://indiaai.gov.in/ai-standards/transparency
[37] https://www.policycircle.org/opinion/big-tech-ai-regulation/

requirement of major investment in regulatory capacity and possibly global cooperation on technical standards for AI auditing.

Policy and Regulatory Implications: The Digital India Act is meant to radically transform India's legal framework into one that is more adaptive, forward-looking, and complete in confronting the intricate legal and policy issues arising from the digital revolution and the advent of Artificial Intelligence.

Its central goal is to achieve an inauspicious equilibrium between inviting innovation and growth without significantly downplaying conceivable adverse effects. The pre-DIA AI regulatory environment in India was dominated by a sectoral, disjointed, and mostly non-binding pattern, with NITI Aayog and MeitY policy documents being advisory in nature as opposed to being legally binding. This led to the absence of horizontal regulation across industries, inadequate safeguarding of core rights against algorithmic damages, and the lack of a clear institutional supervisory mechanism for AI.[38][39][40][41]

The transition from a "soft law" (advisory) to a "hard law" (binding legislation) framework for AI regulation under the DIA marks a significant coming of age of India's digital policy, compelled by the increasing societal effects and harms of AI. The fact that NITI Aayog's AI principles were only "suggestions and policy recommendations" and MeitY's AI Governance Guidelines Report did not bring in "legally binding regulations" is at variance with the expressed desire of the DIA to "upgrade India's legal landscape" and "translate these principles into enforceable clauses." This policy development reflects an appreciation that the disruptive potential of AI and the dire implications for constitutional rights cannot be best addressed through voluntary industry pledges alone. This reflects a strategic shift from an original "innovation-first, regulate-later" approach to a more precautionary "innovation-with-safeguards" approach. This shift, though necessary for user protection and confidence, will necessarily bring higher compliance costs for companies, especially those working with high-risk AI systems.[42]

[38] https://olawebcdn.com/ola-institute/Indias_Digital_Future_Strengthening_DPDP_Rules_for_Privacy_Innovation_and_Global_Leadership.pdf
[39] https://thelondonstory.org/2025/04/15/indias-ai-governance-guidelines-report-faqs-answered/
[40] https://aakashi.hashnode.dev/ai-regulation-in-india-vs-the-world-are-we-ready-or-already-behind
[41] https://singhania.in/blog/ai-and-indian-law-addressing-privacy-ethics-and-copyright-challenges-in-the-digital-age/
[42] https://www.techpolicy.press/indias-ai-governance-guidelines-report-a-medley-of-approaches/

REVIEW OF PROVISIONS OF DIGITAL INDIA ACT

This section offers a comprehensive, section-by-section analysis of the Digital India Act's legislative provisions concerning its approach towards Artificial Intelligence and corollary obligations, as per the user's given text and research material.

Regulating AI Technologies: Provisions and Lifecycle Framework: The Digital India Act (DIA) will supersede the Information Technology Act, 2000, which has been found to fall short of controlling fast-developing technologies like AI. The DIA seeks to create a future-proof structure that encompasses AI tools in its widened definition of intermediaries. One of the key features expected in the DIA is the implementation of "risk-based classification of AI systems." This is a trend that aligns with international best practices, which enable differing regulatory burdens to be applied according to the potential for harm in each AI application.[43][44][45][46]

The MeitY's "AI Governance Guidelines Report," which is of great importance for the DIA, promotes a "lifecycle approach" to the governance of AI. The reason is that it acknowledges that AI risks take different forms along different stages: from development, which includes design, training, and testing; to deployment, which covers operationalisation, possible misuse, and accountability; and then to diffusion, which covers the long-term social effects of broad adoption. The report also investigates "entity-based regulation," or the use of licensing, and "activity-based regulation," or regulation tied to the area of AI application, proposing that the latter is preferable for the mitigation of harm. Additionally, the DIA is anticipated to define "no-go areas" for AI across consumer-oriented applications and recommend severe sanctions for non-compliance, showing a proactive approach towards high-risk applications of AI.[47][48][49]

The prospective adoption of a risk-based classification and a lifecycle methodology marks a shift towards an advanced and responsive regulatory system for AI, recognising that a rigid, one-size-fits-all system does not work for dynamic AI technologies. This methodology provides for a more nuanced and proportionate regulatory response, permitting regulators to allocate resources towards more risky AI applications while promoting lower-risk innovation.

[43] https://www.delhilawacademy.com/digital-india-act/
[44] https://www.upguard.com/blog/digital-india-act
[45] https://thelondonstory.org/2025/04/15/indias-ai-governance-guidelines-report-faqs-answered/
[46] https://millipixels.com/blog/navigating-ai-regulations-in-india-balancing-innovation-and-accountability
[47] https://securiti.ai/ai-governance-in-india-meity-2025-report/
[48] https://www.azbpartners.com/bank/update-on-meitys-report-on-ai-governance-guidelines-development/
[49] https://www.techpolicy.press/indias-ai-governance-guidelines-report-a-medley-of-approaches/

An understanding of the lifecycle is important because AI hazards can present in one form during the early development stage, where discriminatory training data may be input, but in a different form in long-term societal diffusion, which can create systemic bias. The real challenge will be in making these risk categories and stages well-defined but flexible enough to encompass developing future AI innovations while being specific enough for routine enforcement. The long-term success of this paradigm will greatly depend on the regulatory agencies' technical know-how to categorically and track AI systems for their working life, and constant investment in specialised skill sets would be necessary.

Algorithmic Accountability, Transparency, and Non-Discrimination: A core mission of the DIA is to make companies accountable for making their algorithms open and responsible, with specified penalties in case of default. The Act is likely to have provisions to make social media companies accountable for the algorithms they use to display content, to avoid the abuse of Indian citizens' data and even mandate disclosure of data processing practices.

The MeitY's AI Governance Guidelines Report, which provides the DIA with a directive document, focuses on several fundamental principles to ensure this:

Transparency: AI systems need to be open about their capabilities, limitations, and decision-making processes so that users remain informed at all times as to whether they are dealing with an AI system. This principle encompasses encouraging "explainable AI" (XAI) to prevent non-transparent "black-box algorithms".[50]

Equity and Non-Discrimination: AI mechanisms must be equitable, inclusive, and built to avoid discrimination or establishment of biases against a person, community, or group on grounds such as race, caste, gender, religion, or geography.[51]

Human Oversight: Human oversight must continue to be a part of AI systems to avoid negat ive consequences and maintain the rule of law.[52][53][54][55]

[50] https://indiaai.gov.in/ai-standards/transparency
[51] https://thelondonstory.org/2025/04/15/indias-ai-governance-guidelines-report-faqs-answered/
[52] https://www.policycircle.org/opinion/big-tech-ai-regulation/
[53] https://www.nightfall.ai/ai-security-101/algorithmic-accountability-act
[54] https://securiti.ai/ai-governance-in-india-meity-2025-report/
[55] https://www.obhanandassociates.com/blog/legal-perspectives-on-ai-governance-in-india-a-summary-of-the-ai-governance-guidelines-report/

The DIA is expected to require algorithmic explainability and transparency, such as AI bias audits and explanation requirements. Although not AI-specific, the Digital Personal Data Protection (DPDP) Act, 2023, establishes a general framework by defining "automated" processes to presumably cover AI systems and introducing the concept of an "artificial juristic person" to hold them responsible, and thus subject them to data protection regulations such as transparency and accountability.[5657]

The DIA's express emphasis on algorithmic accountability, transparency, and non-discrimination, especially in the case of key decision-making and social media, is an explicit effort to apply constitutional basic rights in the digital space. This effort confronts the stark technical and legal hurdle of how to implement these principles against so-called black-box AI systems. The focus on "algorithmic explainability" and "required bias testing and auditing" addresses the "black-box" challenge head-on, where the inner mechanisms of sophisticated AI models are hard to interpret. This represents a transition from ethical nicety to tangible legal mandates, which is essential for imposing non-discrimination and guaranteeing due process in AI-based decision-making. The success of these measures will hinge on the establishment of good technical standards and mechanisms for auditing and explaining sophisticated AI models and on having highly qualified human capital in regulatory authorities to carry out such audits. The challenge is not merely to identify bias but to assign responsibility and give proper redress when algorithms, not human agents, are the main decision-makers. This can require a reorientation of classical legal evidentiary standards to suit the specific needs of AI.

Data Protection and Security: The Digital India Act (DIA) is intended to supplement the Digital Personal Data Protection (DPDP) Act, 2023, in the regulation of the processing of personal data by AI systems.

The DPDP Act establishes a foundational legal structure for safeguarding digital personal data, emphasising principles of consent, data minimisation, and purpose limitation in data processing. It also possesses extraterritorial applicability, covering data processing outside India if it pertains to offering goods or services within India. The DIA also highlights the need for protection whenever data is crossing borders and points out the role of regulators in creating

[56] https://olawebcdn.com/ola-institute/Indias_Digital_Future_Strengthening_DPDP_Rules_for_Privacy_Innovation_and_Global_Leadership.pdf

[57] https://elplaw.in/leadership/navigating-ai-regulation-in-india-unpacking-the-meity-advisory-on-ai-in-a-global-context/

guidelines to oversee the flow of sensitive or strategic data, at times espousing data localisation to protect Indian economic and strategic interests. MeitY's AI Governance Guidelines Report lays stress on the need for "privacy-by-design" and "security-by-design," i.e., AI systems must naturally embed data protection features from the very beginning.[58]

While the DIA fills out the DPDP Act to form a multi-layered framework of data governance for AI, the exclusion by the DPDP Act of publicly available data from its scope is a major potential loophole for training AI, which has to be addressed by the DIA. The DPDP Act is concerned with personal data, consent, and cross-border data flows. It strictly says, though, that it "does not apply to public data." The strength of AI is based on "vast amounts of data," and much of the AI training, particularly for large language models, comes from publicly available data sets. Exclusion of publicly available information from the regulatory ambit of the DPDP Act directly may enable the AI developers to avoid consent and data protection requirements for such information, creating potential for unintentional privacy consequences or incorporating biases from unfiltered public databases. This is a major area where the DIA might have to make special provisions or regulations on the ethical and privacy concerns of utilising public data used for training AI, though technically outside the immediate scope of personal data protection.[59][60]

Enforcement and Institutional Mechanisms: To efficiently follow through on its policy goals, the Digital India Act institutes new institutional structures. These consist of the Digital India Authority (DIA), the Digital Grievance Appellate Boards (GACs), and a Digital Advisory Council.

Digital India Authority (DIA): It will be an autonomous expert organisation vested with sweeping powers to regulate and oversee the digital space, set codes of practice, hear complaints, and impose penalties for non-compliance.[61] Digital Grievance Appellate Boards (GACs): These appellate boards are meant to be specialist, fair, and accessible forums for appealing platform in-house grievance bodies' decisions. They seek to adjudicate appeals promptly, normally within 30 days.[62]

[58] https://www.thebridgechronicle.com/tech/india-ai-regulation-global-model-2025
[59] https://www.shankariasparliament.com/current-affairs/digital-india-act-2023
[60] https://www.bricscompetition.org/news/digital-india-act-sould-include-provisions-making-social-media-companies-accountable-for-algorithms-they-use
[61] https://accesspartnership.com/the-key-policy-frameworks-governing-ai-in-india/
[62] https://informatics.nic.in/news/1455

Digital Advisory Council: This council, made up of industry, civil society, academic, and government representatives, will counsel regulators and lawmakers on policy changes and upcoming legislation.

The DIA confers considerable powers of enforcement upon regulators, such as imposing considerable monetary fines, including revenue-proportional fines, as well as suspending services for repeated violations. Regulators are also permitted to instruct the removal of unlawful content, suspend individual accounts, or temporarily disconnect services. In addition, they can initiate criminal penalties for serious or wilful violations, fraud, or activities posing risks to public order and child protection.

The establishment of expert, nominally independent institutional bodies such as the Digital India Authority and GACs is an important step towards successful AI regulation, but how truly independent they are, how technically proficient, and whether they can compel even powerful worldwide tech companies will be the final test of their success. The focus on "expertise" and "independence" is crucial in establishing confidence in the operation and oversight of sophisticated AI systems, particularly in light of the "competence gap" within current regulatory institutions.

The accelerated resolution timescale for GACs is bold but essential in allowing for timely redressal to citizens impacted by algorithmic outcomes. But the actual efficacy of these institutions will depend on several factors: their actual functional independence from political interference, a point of concern with the DPDP Act; their capacity to recruit and retain the best technical expertise to appreciate, audit, and regulate complex AI technologies; and their effectiveness in enforcing orders and imposing penalties on large, well-funded multinational corporations likely to engage in jurisdiction-defying or compliance-resistant behaviour. Without these factors, the ambitious aspirations of the DIA risk being undercut by practical constraints.

Digital India Act: AI-Specific Provisions and Obligations

Key AI Governance Area	Specific DIA Provision/Expectation	Objective/Impact	Relevant Snippet IDs
Expanded Definition of Intermediaries	Includes AI tools, gaming apps, and other emerging technologies.	Holds a broader range of digital platforms and AI providers accountable for the content and user safety.	
AI & Deepfake Regulation	Special provisions to regulate AI-generated content, especially deepfakes, misinformation, and biased algorithms, mandate clear labelling of AI-generated content.[63]	Prevents dissemination of harmful AI-generated content, enhances transparency, and combats misinformation.	
Algorithmic Accountability	Places duties on firms to design and implement algorithms openly and responsibly [User Query]. Social media companies are to be accountable for the algorithms used for content presentation.	Ensures responsibility for AI-driven decisions, prevents misuse of data, and promotes ethical AI development.	User Query,
Transparency (Algorithmic Explainability)	Requires disclosure of AI capabilities, limitations, and decision-making processes; promotes Explainable AI (XAI).	Avoids "black-box" algorithms, builds user trust, and enables scrutiny of AI decisions.	User Query,

[63] https://elplaw.in/leadership/navigating-ai-regulation-in-india-unpacking-the-meity-advisory-on-ai-in-a-global-context/

	Mandate transparency norms for explainable AI [User Query].		
Fairness & Non-Discrimination	AI systems must be fair, inclusive, and designed not to discriminate or create biases against individuals/groups. Aims to bar and punish algorithmic discrimination [User Query].	Safeguards fundamental rights, prevents the perpetuation of societal inequalities, and ensures equitable access to services.	User Query,
Risk-Based Classification of AI	Expected to include risk-based classification of AI systems (e.g., low-risk, high-risk).	Allows for proportionate regulation, focusing stringent oversight on AI systems with higher potential for harm.	
Human Oversight	AI systems must remain subject to human intervention, judgment, and oversight.	Prevents adverse outcomes, respects the rule of law, and maintains human control over critical decisions.	
Data Protection & Privacy	Complements the DPDP Act, 2023, for regulating personal data by AI. Emphasises privacy-by-design and security-by-design. Calls for data localization for sensitive/strategic data [User Query].	Ensures lawful processing of personal data, protects user privacy, and secures national interests.	User Query,

Institutional Oversight	Establishes Digital India Authority (DIA) for regulation and monitoring [User Query]. Proposes an AI incident database for tracking failures and risks.	Centralised AI governance enhances regulatory capacity and provides a mechanism for learning from AI-related harms.	User Query,
Grievance Redressal	Creates Digital Grievance Appellate Boards (GACs) for appeals from platform decisions [User Query]. Strengthens grievance redressal systems tailored to digital industries.	Provides accessible and expert channels for users to contest AI-driven decisions and seek redress.	User Query,
Enforcement Powers	Grants regulators powers to levy substantial monetary fines, suspend services, direct content removal, and initiate criminal sanctions [User Query].	Ensures compliance, deters violations and provides legal recourse against non-compliant entities.	User Query

COMPARATIVE REVIEW

This section critically assesses India's Digital India Act response to AI regulation in contrast to leading international regimes, notably the EU Artificial Intelligence Act and the USA Algorithmic Accountability Act, and examines areas of convergence, divergence, and specificity.

EU Artificial Intelligence Act: The EU AI Act is broadly accepted as the global first all-encompassing legislative framework for AI regulation, embracing a strict risk-based categorisation framework. The Act categorises AI systems into four risk levels:[646566]

[64] https://www.trail-ml.com/blog/eu-ai-act-how-risk-is-classified
[65] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
[66] https://www.softwareimprovementgroup.com/eu-ai-act-summary/

Unacceptable Risk: Such systems are categorically prohibited because they inherently pose a threat to basic rights. These include AI for cognitive behaviour manipulation, social credit scoring, and real-time remote biometric identification in public areas, with extremely narrow exemptions for law enforcement under severe conditions. The ban on unacceptable risks came into force in February 2025.[67]

High Risk: These are systems that have a significant effect on safety or basic rights. They are subject to thorough evaluation both before being made available on the market and ongoing during their entire lifecycle. High-risk AI systems need to be registered on an EU database and meet an extensive set of criteria such as strong quality management systems, data governance practices, cybersecurity, and verifiable accuracy and resilience. Examples encompass AI in the management of critical infrastructure, education, employment, essential services, law enforcement, and migration. High-risk system obligations are to take effect 36 months from the entry into force of the Act.

Limited Risk: This type mainly includes generative AI models such as ChatGPT. Although they are not considered to be inherently high-risk, they fall under certain transparency obligations. Providers have to declare when content is AI-generated, put in place processes to avoid generating illegal content, and publish overviews of copyrighted material used for training. Deep fakes, as an example, need to be labelled as AI-generated.

Low Risk: The majority of AI systems in this group, including spam filters, have no specific duties under the Act, though there is encouragement of voluntary codes of conduct.

For enforcement, EU AI Act prescribes significant fines for non-compliance. Maximum fines may extend up to €40 million or 7% of global turnover per year for unlawful use of AI, and €20 million or 4% for data or transparency breaches.

The EU AI Act's prescriptive, risk-management approach, coupled with its heavy focus on core human rights and pre-emptive prohibitions, is creating a global regulatory standard that India is following and taking cues from at least, although eventually, it will have a different regulatory philosophy.

The repeated characterisation of the EU AI Act as "the world's first global AI law" with a "risk-based system of classification," encompassing flat prohibitions of "unacceptable risk" AI and

[67] https://www.modelop.com/ai-governance/ai-regulations-standards/eu-ai-act

tight controls on "high-risk" systems, and its high-level penalties specified, demonstrates its pioneering and strength-based nature. This forward-looking and prescriptive regulatory approach, especially its emphasis on core rights and security, makes the EU a major global rule-maker.

India's consistent benchmarking with the EU AI Act, attested by scores of mentions in its policy papers, suggests that while India prefers a "light-touch" or innovation-centric strategy, the EU's detailed framework is an important yardstick to measure possible risks and associated safeguards. This further implies that EU companies in India, or Indian firms handling EU data, will have to navigate both regulatory regimes, possibly resulting in a "Brussels Effect" in which EU regulations become de facto global standards for some AI uses because of their extensive extraterritorial application.

USA Algorithmic Accountability Act: The Algorithmic Accountability Act (AAA) is a legislation bill in the USA designed to counter the threats from AI-based systems in "critical decision-making" processes that have a substantial impact on people's lives.

Such critical decisions include fields like health, money, jobs, housing, and educational prospects. The primary emphasis of the AAA is to establish new transparency on when and how AI systems are deployed and to enable consumers to make well-informed decisions when they engage with them.[686970]

The AAA sets a minimum standard for businesses to perform impact assessments before and after deploying automated critical decision-making processes. The FTC must develop regulations that lay out orderly guidelines for the assessments as well as reporting. Businesses must report specific impact assessment reports to the FTC, which will annually publish an anonymised aggregate report detailing trends.

The FTC is also charged with creating a public repository in which advocates and consumers can view automated critical decisions, such as data sources, high-level metrics, and how to appeal decisions. In addition, the Act requires consultation with stakeholders, mitigation of

[68] https://www.congress.gov/bill/117th-congress/senate-bill/3572
[69] https://www.wyden.senate.gov/imo/media/doc/algorithmic_accountability_act_of_2023_summary.pdf
[70] https://www.nightfall.ai/ai-security-101/algorithmic-accountability-act

adverse effects, privacy risk assessment, ongoing performance testing (including differential performance testing based on consumer factors), and employee training.[71][72]

For enforcement, the AAA suggests augmenting the FTC with resources in the form of 75 new employees and the creation of a Bureau of Technology. This new bureau would be charged with enforcing the provisions of the Act and facilitating the Commission's technological operations.

The USA's Algorithmic Accountability Act, with its focus on impact assessments and transparency for "critical decisions," embodies a market-regulatory philosophy of looking to disclosure and consumer empowerment as the means for accountability. It is possible that this would be more aligned with India's pro-innovation approach than the EU's rule-based approach.

The AAA's fundamental mandate for "impact assessments" and "new transparency" for AI systems in "critical decision-making" seeks to empower consumers to make knowledgeable decisions and depends on the FTC for enforcement. This method is less on the pre-emptive bans or pure technical compliance, as in the EU, and more on making companies comprehend and reveal the effects of their AI systems, making it possible for post-deployment regulation and redress.

The creation of a "Bureau of Technology" at the FTC recognises the imperative need for technical expertise in regulatory agencies to properly regulate AI, one that India too is grappling with. Such a model could be especially appealing to India because it opens up more flexibility in developing AI while maintaining accountability and transparency mechanisms, something possibly attuned to India's aspiration to encourage innovation.

Convergence, Divergence, and Unique Aspects: A comparative analysis of India's Digital India Act (DIA) vis-a-vis the EU Artificial Intelligence Act and the USA Algorithmic Accountability Act presents considerable convergences, divergences that are unique to each, and unique features specific to India's regulatory doctrine.

[71] https://www.billtrack50.com/billdetail/1448174
[72] https://www.congress.gov/bill/118th-congress/house-bill/5628/text

CONVERGENCE

Each of the three schemes shows an understanding of the transformative powers and inherent risks inherent in Artificial Intelligence. They all meet on fundamental ethical and legal tenets, such as the need for transparency, accountability, equity, and the elimination of bias and protection of privacy in artificial intelligence systems.

Commonality of views among these jurisdictions is also in the recognition of the need for human control of AI-driven decision-making, recognizing that artificial intelligence systems must not be completely autonomous, particularly in high-risk situations. The common emphasis on transparency, for example, is a testament to a worldwide consensus that users must be able to comprehend how AI systems work and when and to what extent they are engaging with them, trending toward "explainable AI" as the norm.

DIVERGENCE

There are still important divergences, however, including in regulatory philosophy and practice:

Regulatory Philosophy: India's style, as manifested in the DIA, has typically been described as "pragmatic and context-sensitive" to walk a tightrope that is neither "overregulation," potentially suffocating innovation and entrepreneurship, nor "under regulation," potentially allowing free rein to abuse. It is focused on "principles-based guidance and self-regulation by industry" and tends towards a "light-touch" regulatory approach. This is in stark contrast to the EU's "prescriptive AI-specific legislation" and "risk-based regulatory approach," which entails strict legal requirements, pre-emptive prohibitions on the use of particular AI applications, and severe sanctions in case of non-compliance. The USA's AAA, though detailed in its demands for impact analysis and transparency, is more focused on "critical decision processes" and excels in disclosing and monitoring after deployment than with sweeping risk categorization and pre-market clearance.[73][74]

Binding Nature: While the DIA aims to be a legally binding framework, India's pre-DIA AI governance largely consisted of advisory guidelines and policy recommendations, lacking

[73] https://thelegalwire.ai/from-techno-regulation-to-ai-safety-research-indias-ai-governance-landscape-in-2024/
[74] https://elplaw.in/leadership/navigating-ai-regulation-in-india-unpacking-the-meity-advisory-on-ai-in-a-global-context/

direct enforceability. In contrast, the EU AI Act is a fully legally binding instrument with clear compliance timelines and substantial fines. The USA AAA has currently proposed legislation, indicating a move towards binding regulation, but it has not yet been fully enacted.

Scope and Implementation: The EU AI Act is universal in scope across many sectors and risk levels, covering widely applicable AI systems. India's DIA is similarly expansive, substituting the IT Act and addressing a broad digital landscape, with dedicated provisions for AI. The USA AAA is more targeted towards particular "critical decision processes" that have substantial impacts on customers' lives, as opposed to a general categorisation of all AI systems.

Distinctive Features of India's Approach: India's response to AI governance is informed by its distinctive national context, resulting in several distinctive features:

Scale and Diversity: The huge and heterogeneous population of India, and its fast-paced digital growth, introduce specific challenges and possibilities for AI implementation, especially in public welfare programs and digital divide bridging efforts. The sheer scale of the users and transactions demands scalable and inclusive regulatory frameworks.

Constitutional Values: There is a strong focus on ensuring that AI development and deployment in India is consistent with Indian constitutional values, basic rights like privacy, non-discrimination, and due process, and wider public interest. This involves addressing particular domestic issues like caste-based discrimination, which could be fuelled by discriminatory algorithms.

"Digital Nagrik Rights": The idea of a "Digital Bill of Rights" for users, both rights and obligations, presents a balanced view of digital citizenship, intending to create a responsible digital environment where users are also held responsible for their online behaviour.

Data Localisation: The DIA and associated policies focus on data localisation for sensitive or strategic data, which indicates national sovereignty concerns and a need to safeguard Indian strategic and economic interests by having direct control over vital information.

"Techno-legal" Strategy: India's strategy is to utilize digital technology for governance, including automated compliance software and possibly "consent artifacts" to facilitate greater traceability and attribution of liability. This strategy attempts to integrate legal provisions into

technology itself, similar to "privacy by design," to achieve compliance in a rapidly changing technology scenario.

India's "light-touch" and "balanced" approach, although having the potential to encourage innovation, runs the risk of instilling regulatory uncertainty and a weaker enforcement climate than the EU, particularly if it is based excessively on voluntary as opposed to legally enforceable commitments for high-risk AI. The term "pragmatic" and avoiding "overregulation" used to describe India's approach implies a conscious policy to encourage AI development. Yet, in contrast, criticism suggests that "self-regulation and voluntary commitments are not enough" to attain the requisite accountability and transparency levels, especially with the potential for disruption inherent in AI. The absence of "strict AI bias and explainability laws" compared to the EU might result in a less strict enforcement regime being perceived. This "light-touch" approach, while perhaps desirable for stimulating AI progress and investment, may create a "competence gap" in regulatory bodies and a possibility of "compliance theatre and legal evasion" by dominant tech players. The lack of definite, legally enforceable standards for some AI uses may expose citizens to harm, especially that resulting from algorithmic bias or transparent decision-making, without access to clear mechanisms for remedy. India's success in the long run will thus depend on how it can move from aspirational principles to tangible, enforceable provisions, especially for high-risk AI systems. This needs a robust regulatory design that can keep up with fast-changing technology, while providing effective protection of basic rights.

DISCUSSION AND RECOMMENDATIONS

The examination of the Digital India Act (DIA) from an AI governance perspective identifies a visionary legislative initiative to confront the intricacies of the digital era beyond the constraints of the ageing Information Technology Act, 2000. The DIA evidences no doubt about an explicit desire to encourage responsible AI development on the professional principles of accountability, transparency, and non-discrimination and enacts new institutional arrangements for regulation. There are some potential gaps and limitations which should be noted.

This part will cover these fields and suggest concrete policy and legislation reforms to make the DIA more effective in AI regulation. 4.1. Shortcomings and Loopholes in the DIA's AI

Framework. Although its purpose is forward-thinking, the DIA's AI framework has several fields that can be improved to provide full and proper regulation:

RISK CLASSIFICATION

Ambiguity and Enforcement: Although the DIA is supposed to implement a risk-based classification for AI systems, the exact definitions of "high-risk" and the related strict obligations are not yet completely detailed in publicly accessible information. Lacking transparent, legally binding definitions and detailed requirements for each risk category, risk of regulatory uncertainty for developers and deployers. In addition, if the adherence to these categories of risk depends primarily on voluntary commitment, as a few MeitY reports have indicated for more general AI governance, then the effectiveness and enforceability of the framework, particularly for high-risk AI, may be watered down. This method might result in a weaker regulatory regime than the EU AI Act's prescriptive approach, with its high punishments.

Challenges in Algorithmic Explainability and Bias Reduction: The DIA requires transparency and algorithmic bias reduction. Yet, mandating effective "algorithmic explainability" for sophisticated "black-box" AI models, especially deep learning models, is a huge technical challenge. The existing legal infrastructure, even with the DIA, might not be able to force companies, especially multinationals, to open up completely proprietary algorithms or to come up with explanations understandable to ordinary people or even regulators. The lack of clear, thorough requirements for mandatory testing for bias, independent audits, and ongoing observation of AI systems, as well as explicit provisions in the law for redress in instances of algorithmic discrimination, may expose citizens to danger.

Publicly Available Data Coverage for AI Training: Although the DPDP Act and the DIA seek to protect personal data, the exclusion of publicly available data under the DPDP Act's direct regulatory purview leaves a probable loophole for AI training. AI systems often train on large public datasets, which, being uncurated or biased, might perpetuate social biases or cause privacy violations by inference even without processing directly identifiable personal data. The

existing framework does not necessarily cover the ethical and privacy consequences of such data being used for developing AI systems.[757677]

Institutional Capacity and Technical Expertise: The creation of the Digital India Authority and Digital Grievance Appellate Boards is a good move towards sole oversight [User Query]. But such effectiveness depends on their actual autonomy from political interference and recruitment and retention of highly specialised technical talent in AI, data science, and cybersecurity. Lacking sufficient technical capability, such regulators can fail to comprehend, audit, and enforce regulations successfully against advanced AI systems created by well-funded global technology giants, risking "regulatory capture" or ineffective oversight.

Cross-Border Enforcement and Jurisdiction: The DIA recognises the difficulty of multinational AI companies in India [User Query]. In asserting India's legal jurisdiction and policy goals, however, the real mechanisms of enforcement to compel compliance, provision of data for investigations, and enforcement of penalties against foreign actors are problematic. A balance between compliance with international standards and addressing unique domestic circumstances must be carried out carefully in order not to create conflicts of law or diplomatic tension.

Intellectual Property Rights Over AI-Generated Content: The accelerated spread of AI-generated content (e.g., text, photos, deep fakes) creates sophisticated problems of copyright ownership and infringement.

The existing Indian legal framework, comprising the IT Act and the Copyright Act, doesn't specifically cater to AI-generated content, and thus, there is a huge legal vacuum as far as authorship claims and using copyrighted data to train AI are concerned. This vagueness can impede innovation (by discouraging AI developers) and content protection (for original developers).

Policy and Legal Reforms: To fill the identified gaps and improve the Digital India Act's ability to provide effective governance for AI, the following policy and legal reforms are suggested-

[75] https://millipixels.com/blog/navigating-ai-regulations-in-india-balancing-innovation-and-accountability
[76] https://law.asia/india-ai-regulation-focus-unified-approach/
[77] https://www.barandbench.com/view-point/the-confluence-of-ai-and-data-privacy-aligning-data-privacy-regime-in-india-for-the-age-of-ai

Fine-grained Risk-Based Categorisation with Defined Obligations:

Reform: The DIA must include a thorough, legally enforceable system for AI risk classification with a clear description of "unacceptable," "high," "limited," and "minimal" risk categories, learning from the EU AI Act. For "high-risk" AI systems, specific and clear obligations should be required, such as:

Mandatory Conformity Assessments: Mandating that AI developers and deployers perform independent third-party conformity assessments before high-risk AI systems being put on the market or deployed, and at regular intervals thereafter.

Robust Risk Management Systems: Mandating the use of robust risk management systems across the AI lifecycle, from design to diffusion, with explicit procedures for the identification, assessment, and mitigation of risks.

Data Governance Requirements: Defining strict data governance requirements for high-risk AI, such as data quality, representativeness, and bias reduction measures for training data.

Effect: This will deliver legal certainty, ensure proportionate regulation, and concentrate enforcement efforts on areas where there is the greatest potential for harm, while enhancing innovation in lower-risk uses. It goes further than voluntary guidance to enforceable legal obligations.

Enhanced Algorithmic Transparency and Bias Reduction Mechanisms:

Reform: The DIA ought to require clear standards for algorithmic explainability and transparency, especially for AI systems that issue "critical decisions" affecting rights or the ability to access services. This should involve:

Forced Impact Assessments: Demanding thorough algorithmic impact assessments (AIAs) for high-risk AI systems, like the USA's Algorithmic Accountability Act, to detect and counteract possible biases or discriminatory impact.[78][79]

[78] https://www.wyden.senate.gov/imo/media/doc/algorithmic_accountability_act_of_2023_summary.pdf
[79] https://www.congress.gov/bill/118th-congress/house-bill/5628/text

Explainability Standards: Establishing technical standards for explainable AI (XAI) to make AI decisions comprehensible to impacted persons and regulators, preventing "black-box" results.

Bias Audits and Testing: Enforcing frequent, third-party bias audits and thorough testing of AI models, particularly those deployed in high-stakes fields such as finance, healthcare, and law enforcement, to actively detect and correct for discriminatory results.[80]

Right of Explanation and Contestability: Itself codifies a "right of explanation" for those who are impacted by automated decisions and strong processes to contest, rectify, or appeal those decisions, and with due process.

Effect: These will improve accountability, empower citizens, and actively mitigate the risk of algorithmic discrimination, placing AI systems in sync with India's constitutional values of equality and non-discrimination.

Controlling Publicly Available Data for AI Training:

Reform: The DIA must bring in provisions or guidelines on the specific ethical and privacy implications of utilising publicly available data for AI training, even where such data is not within the DPDP Act's definition of "personal data." This can include:

Ethical Sourcing Guidelines: Creating guidelines for the ethical sourcing and curation of public datasets used for AI training, concerning representativeness, quality, and preventing embedded biases.

Data Provenance Transparency: Mandating AI developers to be transparent about the provenance of data employed for training, such as whether it was sourced from the public and steps taken to use it ethically.

Impact: This will fill a regulatory gap, avoid passing on biases within uncultivated public data, and guarantee an all-around data ethics approach to AI development.

[80] https://olawebcdn.com/ola-institute/Indias_Digital_Future_Strengthening_DPDP_Rules_for_Privacy_Innovation_and_Global_Leadership.pdf

Strengthening Institutional Capacity and Technical Capabilities:

Reform: A major investment must be made to strengthen the technical capability and autonomy of the Digital India Authority and the Digital Grievance Appellate Boards. This should involve:

Recruitment of AI/Tech Experts: Actively recruiting and retaining an elite team of highly qualified AI, data science, and cybersecurity professionals in such regulatory forums.

Dedicated AI Governance Unit: Creating a dedicated AI governance unit under the Digital India Authority, which would be well-resourced with sophisticated AI auditing tools, testing mechanisms, and monitoring systems.

Training and Collaboration: Sustaining ongoing training for regulators about the latest AI technologies and engaging with academia, research institutions, and global AI governance forums to exchange information and best practices.

AI Incident Database: Institutionalising the suggested AI incident database to gather and analyse AI harm information systematically to inform evidence-based policy interventions and cultivate a culture of accountability.

Impact: A technically expert and unbiased regulatory agency is critical for effective regulation of sophisticated AI systems, making sure that regulation is pragmatic, enforceable, and responsive to fast-paced technological innovation.

Enhancing Cross-Border Enforcement and Cooperation:

Reform: To properly regulate multilateral AI companies, the DIA must investigate means of enhancing cross-border enforcement and international cooperation:

Bilateral/Multilateral Agreements: Negotiating bilateral or multilateral agreements with major jurisdictions (e.g., EU, USA) on AI regulation, data sharing for regulatory purposes, and mutual enforcement support.

Clear Extraterritorial Provisions: Securing that the extraterritorial provisions of the DIA are explicit and strong, providing for the exercise of jurisdiction over foreign entities offering AI services to Indian nationals.

Data Localisation Nuances: While data localisation is an expressed priority, it should be balanced by a nuanced consideration of national security needs versus the requirements of global AI development and cross-border data flows, possibly by secure data mirroring or trusted data flows under stringent terms.

Impact: This will strengthen India's power to hold foreign AI entities responsible, ensure compliance with Indian laws, and assist in the formation of harmonised global AI regulation standards.

Enabling Intellectual Property Rights for AI-Generated Content-

Reform: The DIA, or complementary legislation, must address the intellectual property effects of AI clearly:

Authorship and Ownership: Give unambiguous legal directives on the authorship and ownership of works produced by AI systems, taking into account the extent of human contribution to their creation.

Copyright Infringement in Training: Create explicit regulations on the use of copyrighted works for training AI, with provisions for fair use, licensing, or obligatory compensation mechanisms for right holders.

Content Provenance: Mandate content provenance systems, including digital watermarking or metadata, on AI-based content to track the source and differentiate it from human-generated content, particularly for deep fakes.[81]

Effect: This will offer legal certainty to creators and developers, ensure innovation in AI-generated content, and safeguard the rights of original copyright holders from possible disputes.

CONCLUSION

The Digital India Act represents a pivotal legislative endeavour poised to modernise India's digital governance framework, specifically addressing the profound implications of Artificial Intelligence. Building upon foundational policy initiatives like NITI Aayog's aurorally and

[81] https://elplaw.in/leadership/navigating-ai-regulation-in-india-unpacking-the-meity-advisory-on-ai-in-a-global-context/

MeitY's AI Governance Guidelines, the DIA aims to establish a comprehensive, future-proof legal regime that balances innovation with robust safeguards for user rights and societal well-being. The Act's proposed provisions of risk-based AI classification, increased algorithmic accountability, transparency, and non-discrimination, along with the introduction of specialised institutional bodies such as the Digital India Authority and Digital Grievance Appellate Boards, represent a shift in strategy from a disjointed, advisory-based regime to a binding, enforceable legal regime.

Comparative examination with international benchmarks, in particular the EU AI Act and the USA Algorithmic Accountability Act, also brings out convergence on general ethical principles as well as divergence in regulatory philosophies. Where Indian policy endeavours to find a balanced approach, neither too much nor too little regulation to promote its emerging AI ecosystem, the prescriptive stance of the EU Act and the USA Act's transparency-oriented requirements provide lessons. The peculiar issues presented by India's large and heterogeneous digital populace, compounded by the presence of multinational AI developers, further highlight the need for a regulatory framework that is not only strong but also fluid and extraterritorially enforceable.

Even with its lofty goals, the success of the DIA will depend on whether the aspirational ideals can be translated into tangible, binding legal requirements, especially for AI applications at high risk. Resolving the risk classifying ambiguities, enhancing the algorithmic explainability mechanisms and bias reduction efforts, clarifying the legal standing of publicly available data used for AI training, and greatly increasing the technical capability and autonomy of regulatory agencies are paramount to the success of the DIA. Additionally, taking the initiative to define intellectual property rights for AI-generated material and encouraging international cooperation will be vital in empowering India to exercise its digital sovereignty and assume a responsible role in being a leader of the global community of AI nations. Through consistent enactment of these reforms, the Digital India Act will realise its vision of having an open, secure, and innovative digital space that truly reflects the republic.