IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

REGULATING AI: A COMPARATIVE ANALYSIS OF INDIA AND GLOBAL FRAMEWORKS[1]

[1]Sonasri.S 1st Author, [2]M. Blessy Priya Niranjana 2nd Author,
[1]Assistant professor, [2]Assistant Professor,
[1]Law 1st Author,
[1]Bharath Institute of Law 1st Author, Chennai,India

Abstract: The rise of AI systems raises concerns about privacy violations, data breaches, and unauthorized use of sensitive information. To address these concerns, the European Union (EU) enacted the Artificial Intelligence Act. On December 9, 2023, the EU entered into a provisional agreement to prohibit the use of AI in cases where it may harm citizens' rights. To establish an ethical framework for AI, it is important to explain the risks and opportunities associated with its design and use. The goal is to create an ecosystem that maximizes opportunities while minimizing risks. An ethical approach provides a dual advantage for AI developers and start-ups, allowing them to harness social value by taking advantage of new opportunities that society values. In India, artificial intelligence is still in its early stages due to the country's development status. This technology is ascribed to technical advancements in the 21st century, including the advent of social networking sites and global firms' investment in India began research and development in the field of artificial intelligence. As we see this emerging amazing technology that operates on the human thought process. Today, we may observe the global application of artificial intelligence in all sectors of the economy. It has not only reduced the strain, has also boosted workplace efficiency using smart technology. So, this research paper will focus on the laws which protects the data and will compare this study with other country data protection laws. The article will explore the challenges faced by businesses and policymakers in balancing innovation with privacy rights, as well as the opportunities for creating a robust data protection regime that fosters trust in AI applications.

Index Terms - Data Protection, Artificial Intelligence, ethics, policies, laws, EU, business.

[1] Author Sonasri S, Assistant Professor, Bharath Institute of law & Co- Author Blessy Priya Niranjana Assistant Professor, Bharath Institute of law.

I. INTRODUCTION

Artificial Intelligence (AI), which aims to emulate the cognitive processes of the human brain for problem-solving or simply for learning, possesses the potential to revolutionize nearly every facet of human life. This aspect of intelligence is often referred to as machine intelligence, where machines are designed to exhibit behaviors that contrast with the natural intelligence of humans. AI is consistently advancing to offer benefits across a variety of industries. These machines are developed through a multidisciplinary approach that incorporates fields such as mathematics, computer science, linguistics, psychology, and more. AI has permeated numerous fields and sectors including finance, banking, smart cities, transportation, healthcare, education, agriculture, and many others are beginning to join this trend. The safeguarding of personal data is rapidly becoming one of the most significant challenges of our generation. The G20 Leaders Declaration emphasized that innovation is a crucial driver of economic growth, which can also foster inclusivity. We will strive towards creating an inclusive, sustainable, secure, trustworthy, and innovative society through digital advancements and the promotion of emerging technologies. We resonate with the vision of a human-centered future society, championed by Japan as Society 5.0[2]. AI is reshaping society in ways that were once relegated to the realm of science fiction. As digital transformation affects every sector of our economies and societies, we acknowledge the pivotal role of effectively utilizing data as a catalyst for economic growth, progress, and social well-being. The notion that AI is a recent phenomenon is quite misleading. It has been integrated into traffic lights, urinals, vehicle manufacturing, and utilized by pilots in aviation, among other applications, for over a decade. The new economy is expected to adopt AI across various roles and functions traditionally performed by humans. These systems, though not all, can also collect and utilize personal data. The balance between data protection and AI is further complicated by the regulatory strategies employed by different nations[3]. Firstly, AI has predominantly been governed by market forces thus far, with minimal government regulation establishing baseline standards in new and emerging sectors. Secondly, data protection laws, being a relatively new addition to the regulatory landscape, serve a specific purpose of providing control and safeguarding personal data. Thirdly, there remains ambiguity within the legal framework regarding where accountability lies in the context of AI. For instance, if one were to apply criminal law principles to AI and data protection, it necessitates both a mental component and a corresponding action. Machine learning AI incorporates a mental aspect and executes an action. For example, if a dog attacks and kills a person, the dog's owner is held accountable, and the dog may be euthanized (acting through another). Additionally, consider the situation where an AI-governed robot causes the death of a human – who bears the responsibility for that act? Is it the AI's manufacturer? Could it fall upon the programmer? So, who is responsible when a robot collects and utilizes personal information? Numerous parallels exist between self-driving automobiles, robots, and other artificial intelligence systems that have the potential to collect personal information. Kingston uses the example of speeding in a self-driving car to demonstrate how it is a strict liability infraction. Therefore,

[2] Japan Times, Full text of the G20 Osaka leaders' declaration, last accessed on 28.03.2025 https://www.japantimes.co.jp/news/2019/06/29/national/fulltext-g20-osaka-leaders-declaration/#. XTu6qWVeK8U

[3] To further promote innovation in the digital economy, we support the sharing of good practices on effective policy and regulatory approaches and frameworks that are innovative as well as agile, flexible, and adapted to the digital era, including through the use of regulatory sandboxes.

this paper makes the case that the present definition of personal data and idea of consent may not be sufficient in AI where the human interface or control is involved.

LEGAL FRAMEWORK ON DATA PROTECTION LAWS IN INDIA:

Until the year 2023, India lacked an independent law or framework for regulating data protection. The foundation for the data protection framework was built upon the Information Technology Act of 2000 (IT Act) and the associated rules. This encompassed the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

In 2017, a constitutional bench consisting of nine justices from the Supreme Court of India, in the case of Justice K. S. Puttaswamy (Retd.) v. Union of India [Writ Petition No. 494/2012][4], affirmed that privacy is a fundamental right embedded within Article 21 [Right to Life & Liberty] of the Indian Constitution. This ruling initiated the development of a comprehensive data protection framework for the country. After publishing various drafts of the proposed legislation and evaluating feedback from numerous stakeholders, the Ministry of Electronics and Information Technology (MeitY), Government of India, unveiled the draft of the Digital Personal Data Protection Bill in 2022 (DPDP Bill).

The version of the DPDP Bill that was ultimately approved by both chambers of the Indian Parliament included several notable modifications to the initial draft. On August 11, 2023, the Government of India announced this version as the Digital Personal Data Protection Act, 2023 (DPDP Act), which will establish the personal data protection and regulatory framework in India. The DPDP Act introduces various compliance requirements concerning the collection, processing, storage, and transfer of digital personal data. However, additional actions by the Government are necessary to enforce the DPDP Act effectively, including the notification of its sections, repealing the Privacy Rules, and establishing the necessary rules and regulations for successful implementation and enforcement of the DPDP Act. The DPDP Act is limited to personal data in digital format and does not cover non-personal or non-digital data. As a result, the collection and management of non-personal data remain unregulated in India at this time.

To clarify, the existing privacy framework is found within the IT Act and the Privacy Rules. While the Government of India has released a draft of the rules under the DPDP Act, the provisions of the Act itself are not yet in effect.

Rules

MeitY published [5]a draft of the Digital Personal Data Protection Rules, 2025 (Draft Rules), and invited public and stakeholder comments until February 18, 2025. The government will consider the feedback received after this date. Rules governing the establishment and operation of the Data Protection Board of India are expected to take effect immediately upon the publication of the rules in the Official Gazette (once the DPDP Act is implemented). For the other rules, a grace period may be allowed for entities to comply, after which these rules will become effective. The timeline for this has not been detailed in the Draft Rules.

The DPDP Act has been formulated based on the following principles:

[4] Justice K. S. Puttaswamy (Retd.) v. Union of India [Writ Petition No. 494/2012].

[5] On January 3, 2025,MeitY published the draft rules in their official website.

- The use of personal data by an organization must be conducted in a way that is lawful, equitable, and clear to the individuals involved;
- The use of personal data should be confined to the purpose for which it was originally gathered;
- Only the specific pieces of personal data necessary to achieve a particular objective should be collected;
- Reasonable measures should be taken to ensure the personal data of individuals is accurate and remains current;
- Data storage must be restricted to the time period necessary for the stated objective for which the personal data was obtained;
- Appropriate safeguards should be implemented to prevent unauthorized collection or processing of personal data, with the aim of averting personal data breaches; and
- The individual who determines the purpose and methods of processing personal data, known as the Data Fiduciary, is responsible for that processing.

Scope and Applicability of the act

The DPDP Act relates to the handling of digital personal data within India, covering cases where personal data is (i) gathered in digital format or (ii) collected in a non-digital format and later converted to digital format. Therefore, the DPDP Act does not cover the processing of personal data in its non-digital form. The term 'personal data' is broadly defined in the DPDP Act to include any information about an individual that can be identified by or in relation to such information. It also describes 'digital personal data' as personal data that exists in digital format[6].

While the DPDP Act applies to Indian organizations engaged in the processing of personal data, it also extends beyond borders, applying to foreign entities that provide goods and services to Data Principals (as defined below) located in India and process personal data in relation to those activities. The DPDP Act does not pertain to (i) personal data used by an individual for personal or household purposes or (ii) personal data intentionally made publicly available by either the Data Principal to whom the personal data pertains or any other person or organization legally required to disclose personal data to the public.

How Artificial Intelligence is Currently Regulated in India?

Information Technology Act of 2000: This legislation grants legal acknowledgment for electronic transactions and establishes guidelines to safeguard electronic data, information, and records from unauthorized or illegal usage. The IT Act 2000, in conjunction with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011, is set to be superseded by the Digital India Act 2023, which is presently in draft stage and is anticipated to encompass essential provisions concerning AI.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021 offers a structure for monitoring social media, over-the-top (OTT) platforms, and digital news outlets. Government

[6] Data protection laws in India, last modified on 6th Jan,2025 and available at https://www.dlapiperdataprotection.com/index.html?t=law&c=IN and last visited on 10th March 2025.

Advisories on AI and Large Language Models (March 2024) stipulate that major platforms must secure approval from MeitY before implementing untested AI models to avert bias, electoral meddling, or indiscernible AI-generated content. However, exemptions are granted to startups and smaller platforms.

Revised guidelines emphasize the necessity for mandatory labelling of unreliable AI models, user alerts regarding content inaccuracies, and mechanisms for detecting deep fakes. The Digital Personal Data Protection Act (DPDP), 2023 serves as the principal law governing data collection, storage, and processing. However, it has limitations, as it does not address AI-specific issues like algorithmic biases or the misuse of AI-generated data, nor does it feature explicit systems for AI auditing or accountability.

Principles for Responsible AI (2021) outline seven fundamental tenets: safety and reliability, inclusivity, non-discrimination, privacy, transparency, accountability, and the promotion of positive human values. There is an encouragement for collaboration among the government, private sector, and research organizations. The National Artificial Intelligence Strategy (2018) was initiated by NITI Aayog under the slogan #AIFORALL. Its focal points include healthcare, education, agriculture, smart cities, and transportation. Recommendations have been acted upon, such as the creation of high-quality datasets and legislative frameworks for data protection and cybersecurity, which serve as a cornerstone for future AI regulation in the nation. The Draft National Data Governance Framework Policy (2022) aims to modernize the collection and management of government data, with the goal of supporting AI-driven research and startups through a comprehensive dataset repository[7].

How can AI Technologies Enhance India's Legal Framework? The timely and efficient administration of justice can be improved with AI, which can optimize case management by automating repetitive tasks such as documentation, case categorization, and scheduling. With more than 5 crore pending cases in Indian courts, AI-powered tools can accelerate processes, allowing judges to concentrate on more critical matters. AI can also examine legal precedents and case laws, providing historical data that supports informed decision-making and the formulation of litigation strategies.

Moreover, AI can aid in the collection, verification, and analysis of evidence, particularly in intricate cases involving substantial datasets, forensic evidence, or digital fraud. The National Forensic Sciences University in Gujarat is incorporating AI to scrutinize digital evidence, thereby speeding up cybercrime investigations. The Tis Hazari District Court in Delhi has launched its inaugural AI-enabled 'Pilot Hybrid Court' equipped with a speech-to-text feature. AI-driven platforms can streamline mediation and arbitration by automating communication and tracking negotiations. Platforms like ODR India utilize AI to enable online dispute resolution[8].

Enhancing Legislative methods: AI can help lawmakers in drafting, studying, and amending regulation by processing widespread quantities of legal and public coverage statistics. AI-driven simulations can expect the social, economic, and environmental impact of proposed laws, enhancing their precision and relevance as an instance, in a few countries, equipment just like the ecu Union's rules modifying Open software program

[7] Greenleaf, G. (2017). Consent in AI Systems: A Global Perspective. International Data Privacy Law, 7(2), 94-109.

[8] AI and India’s Legal Landscape
Available at https://www.drishtiias.com/printpdf/ai-and-india-s-legal-landscape last accessed on 11th March 2025.

(LEOS) are enhanced with AI. AI-powered prison equipment now makes it simpler for folks who aren't attorneys to talk with legal professionals: they might speed up approaches and reduce down at the time needed for prison studies and compliance evaluation progressed regulation.

Enforcement and Crime Prevention: AI can beautify the efficiency of law enforcement by enabling predictive policing, actual-time crime tracking, and evidence evaluation. Currently, Delhi Police used synthetic intelligence (AI) to reconstruct the face of an unidentified homicide sufferer and hired the image on a poster to are trying to find facts approximately his identification the radical method not only brought about the sufferer's identity but additionally played a crucial function in apprehending the perpetrators. Facilitating Compliance with worldwide laws: AI can simplify compliance for multinational companies working in India via analyzing cross-border regulations and exchange legal guidelines automated compliance gear lessen the threat of penalties and enhance India's ease-of doing-business ranking agencies like TCS and Infosys are developing AI compliance tools for global trade agreements. Strengthening company Compliance: AI simplifies felony compliance via automating monitoring, reporting, and filing strategies, especially for agencies running throughout multiple jurisdictions. With India's growing emphasis on ESG (Environmental, Social, and Governance) reporting, AI ensures well timed compliance and prevents violation agencies can use AI for compliance with SEBI's ESG disclosure norms, lowering manual errors. enhancing customer protection Mechanisms: AI can process patron court cases, reveal fraudulent sports, and are expecting marketplace trends to enhance patron protection.

With growing e-trade and virtual platforms, AI permits authorities to cope withgrievances efficiently and prevent fraud. The consumer protection Authority of India can use AI to music unfair alternate practices. Facilitating Environmental law Enforcement: AI can display environmental compliance by using analyzing facts from sensors, satellites, and area reports, ensuring adherence to AI equipment help identify violations which include unlawful mining or deforestation, enabling speedy regulatory action in just four months, the Karnataka Forest department has diagnosed 167 cases of encroachment with the assist of AI-powered evaluation and satellite imagery.

Strengthening intellectual assets Rights: AI tools can streamline IPR techniques by means of supporting in patent searches, drafting, and detecting copyright infringement by using automating complex searches and filings, AI ensures quicker approvals and reduces disputes in IP-in depth industries like pharmaceuticals and IT. With advancements in AI, the U.S. Patent and Trademark office (USPTO) has seen upward thrust in patent applications for AI-assisted inventions, which can be replicated in India.

How Are AI Technologies Impacting India's Legal Framework?

Privacy and Data Protection Risks: AI technologies gather, study, and profit from personal information on a large scale, often lacking proper protections, which jeopardizes the privacy of individuals. The Digital Personal Data Protection Act established in 2023 is a positive move, but it does not have strict enforcement mechanisms, particularly concerning surveillance carried out by AI[9]. Facial recognition technology is widely used in public areas, including its implementation by the police in Hyderabad as part of the Smart Policing

[9] Surden, H. (2019). Artificial Intelligence and Law: An Overview. *Georgia State University Law Review*, 35(4), 1305-1327.

Mission, which raises alarms about widespread surveillance. India ranked second in the world for cyberattacks in 2022, with around 40% of companies employing AI lacking adequate security measures for data.

Unfairness and Discrimination in Algorithmic Decisions: AI technologies frequently amplify social biases stemming from flawed data, resulting in unfair practices in recruitment, lending, and law enforcement. Without clear guidelines to ensure fairness in algorithms, AI continues to sustain existing inequalities, weakening the constitutional values of equality. Reports indicate that AI-based hiring tools in India have been found to disproportionately screen out women from technical positions. In 2018, Amazon halted the use of its proprietary AI recruitment tool due to biases against women, yet similar technologies might still be functioning in India[10].

Intellectual Property Issues: AI raises questions about the core concepts of intellectual property rights by muddling ownership of works created by AI systems. The existing copyright laws in India do not clearly define terms regarding content generated by AI, leaving creators open to exploitation[11]. According to the Copyright Act from 1957, a work can receive copyright protection only if it is original and created by a human being. As a result, works produced by AI do not qualify for copyright. The case of Andersen versus Stability AI Limited demonstrates the risks that artists face due to ambiguous copyright laws.

Economic Disparities and Labor Law Concerns: The rise of AI automation poses a threat to jobs and could worsen economic inequality, challenging the effectiveness of India's labor laws. The Four Labour Codes in India fail to address the issue of job loss resulting from AI advancements. A report from the McKinsey Global Institute suggests that by 2030[12], automation may lead to the displacement of as many as 60 million workers in India's manufacturing industry, with significant impact on sectors like textiles and electronics.

COMPARATIVE ANALYSIS:

The United States currently lacks comprehensive laws to oversee AI. Nevertheless, different governmental departments have initiated efforts to regulate it. At present, the regulation of AI is primarily in the hands of federal agencies, with the White House leading the charge. The Biden administration has developed a framework for an “AI Bill of Rights” for 2022, aimed at guiding government and industry AI use while safeguarding the public against algorithmic bias. As a result, there is still some time before the US establishes official AI legislation. In the meantime, the market forces will continue to navigate the AI landscape in the US.

Conversely, China has been heavily investing in AI and has laid out various strategies to emerge as a global leader in this field by 2030. China possesses one of the most comprehensive AI policies compared to other nations, addressing subjects such as algorithmic recommendations, ethical assessments, and deep synthesis[13]. In August 2023, China introduced new legislation to regulate Generative AI, becoming the first nation to

[10] Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. *California Law Review*, 104(3), 671-732.
[11] Supreme Court of India. (2021). Launch of SUPACE: AI-based Assistance for Judges. Press Release.
[12] Katz, D. M., et al. (2017). A General Approach for Predicting the Behavior of the Supreme Court of the United States. *PLoS One*, 12(4), e0174698.
[13] Jordan Shapiro& Jillian Cota, ‘An Overview of Global Ai regulation and What’s next’ 8 March 2023 https://unctad.org/tir2023#:~:text=China%2C%20the%20most%2Dready%20developing,and%20South%20Africa%20(56) last accessed on 19 March 2025.

explicitly govern this area. These regulations are viewed as quite strict and are likely to have a significant impact on China's domestic AI industry as well as influence the AI policies of other nations that have yet to implement their own AI laws[14].

South Korea, recognized for its advanced technology, aims to establish itself as a global powerhouse in AI. The "AI Act" takes a progressive stance, granting considerable autonomy to users and encouraging innovation without requiring prior government approval. It also lays out ethical guidelines for AI. Furthermore, the government is supporting AI startups and investing in educational institutions to enhance skills related to AI, thereby fostering a conducive environment for artificial intelligence.

The EU's General Data Protection Regulation (GDPR) is a thorough legal framework aimed at ensuring data protection and privacy. Given AI's heavy reliance on data, individuals are at risk of data breaches and security concerns. While the GDPR does not explicitly reference artificial intelligence, it includes provisions relevant to the regulation of AI. The GDPR empowers EU citizens with greater control over their data and outlines rules for its storage and use[15]. Currently, the EU has embarked on creating the "EU AI Act" to provide explicit AI regulation by introducing a "three-tier risk classification model." This model categorizes AI systems based on the potential risks they present to individuals' fundamental rights.

Singapore is one of the pioneering nations to establish a "national AI strategy." As a result, a significant amount of funding has been designated for AI advancement. Recently, it introduced NAIS 2.0, which incorporates Generative AI. NAIS 2.0 has two main goals. The first is to leverage AI for addressing global issues such as climate change and healthcare. The second is to enable individuals and businesses to succeed in the AI landscape. Singapore aspires to evolve into a smart nation, prioritizing AI as a driver for economic growth. In contrast, India's AI policies are more geared towards social progress and inclusivity. While leading economies like the US and China vie for supremacy in AI, India is concentrating on "AI for All."

CONCLUSION:

Implement Comprehensive Legislation Focused on AI: India requires a specific law that tackles challenges associated with AI, encompassing ethical guidelines, accountability frameworks, and risk categorization. The European Union's AI Act, which came into effect in 2024, offers a tiered risk structure for AI applications; India could adopt a comparable method customized for local circumstances. Create an Independent AI Regulatory Body: Establish a centralized organization, similar to the AI Ethics and Governance Authority of India, to supervise the deployment of AI, ensure adherence to regulations, and handle complaints. A dedicated regulatory authority can provide consistency in AI governance across various sectors, minimizing fragmentation and misuse. The UK's Centre for Data Ethics and Innovation serves as an example for promoting ethical AI utilization. Require Algorithmic Accountability and Audits: Implement legislation that obligates AI developers to conduct regular assessments of algorithms to identify biases, inefficiencies, and ethical shortcomings. Algorithmic biases within AI systems used for hiring, lending, or law enforcement can lead to systemic discrimination if left unchecked. For instance, in 2023, the Competition Commission of India raised concerns regarding price discrimination resulting from algorithmic pricing on e-commerce platforms.

[14] Personal Information Protection Law (PIPL), China.

[15] The European Law on Artificial Intelligence https://artificialintelligenceact.eu/the-act/ last accessed on 15th March 2025.

Introduce Bias Impact Assessments (BIA) and Explainability Standards as part of AI lifecycle management in vital sectors such as healthcare and finance. Enhance Cybersecurity Regulations for AI Systems: Formulate strong cybersecurity standards for AI applications to protect sensitive data and defend against AI-fueled cyber threats. CERT-In should require routine vulnerability evaluations and implement AI-specific threat monitoring systems to manage risks effectively. Encourage Responsible AI Practices Through Regulatory Sandboxes: Broaden the implementation of regulatory sandboxes to facilitate controlled experimentation of AI innovations while ensuring safety and compliance. Sandboxes allow for iterative testing and refinement of AI technologies without significant risks. This initiative could begin with the establishment of cross-sectoral sandboxes under NITI Aayog to experiment with AI in fields like healthcare diagnostics, smart cities, and environmental monitoring. Integrate Ethical AI Concepts into Education and Training: Embed ethical AI development and responsible implementation into higher education programs and corporate training initiatives. Educating developers and decision-makers about AI ethics guarantees that future technologies emphasize inclusivity and fairness. Make AI ethics training compulsory for all government-supported AI projects and incentivize private companies to follow suit. Ensure Data Transparency and Access Control: Improve transparency in AI systems by enforcing mandatory disclosures regarding data usage, model training, and decision-making processes. Without transparency, AI systems risk perpetuating opaque decision-making, eroding public trust. Modify the DPDP Act, 2023 to include Right to Explanation provisions, enabling users to comprehend AI-driven outcomes that impact them. Promote Eco-Friendly AI Practices: Advocate for the creation of energy-efficient AI systems to lessen their environmental impact. Training large AI models consumes significant energy, conflicting with India's climate commitments under the Paris Agreement. Offer tax incentives for AI companies adopting green computing practices and establish benchmarks for sustainable AI development.