

Bridging the Ai Governance Gap: Lessons for India's Dpdp Act from the Eu Ai Act and Other Global Standards

Riddhi Rastogi¹, Aniket Dwivedi²

¹Master of Law NIMS University Rajasthan, Jaipur.

²Research Scholar United University.

Abstract

Informational privacy, often called data privacy or data protection, is about a person's to manage how their personal information is composed, used, and shared. Recent AI developments worldwide have captivated many. The Indian population is also experiencing a technological revolution. India is slowly becoming more reliant on technology for most of the services needed in daily life. The use of the internet and the Internet of Things leaves digital footprints that create big data. This data can be both personal and non-personal. Information about individuals can be used to understand their socio-economic profile, culture, lifestyle, and personal details such as love life, health, well-being, sexual preferences, sexual orientation, and various other personal traits. However, issues like data breaches have exposed users to various risks, including cyber crimes and other fraudulent practices. The following queries are addressed in this article's critical analysis of the recently passed Digital Personal Data Protection Act, 2023 (DPDP): How does it handle concerns about data processing and information privacy? What safeguards for information privacy are included in the DPDP Act? How are the state's interests in maintaining national security and safety weighed against individual rights regarding data protection? Can this right be used against non-state actors as well as the state? Following an analysis of the DPDP Act, the paper makes the case for additional enhancements in a number of areas most notably that important choices involving personal information have to be subject to human review to make sure they are not the exclusive product of automated data processing.

Keyword: privacy, personal information, AI developments, worldwide, technological revolution, Internet, Algorithmic Decision-Making, Machine Learning, Predictive Analytics, DPDP Act.

INTRODUCTION

During the recent decades, Artificial intelligence and big language models have brought about overall these are concerns of the common citizen regarding their personal data and privacy. With the development of technology the danger of There is also increased misuse of it. The businesses and the organizations are inventing an increasingly large number of AI products. In this respect or concerns which are pointed out by the citizens, that is why the framework and policy environment of the Artificial Intelligence is it actually took the proportions of becoming a very significant concern of all the jurisdiction around the world comprising of

all the international accompaniments such as firms and organizations like IEEE (Institute of Electricals and Electronics Engineers).¹ OECD (Organisation for Economic Co-Operation and Development). Framework of this research paper shall comprise of; developing and comprehending the realization of Artificial Intelligence, researching on the existing comparing legislations of other jurisdiction, and making legislations in force in India recommendations to conceptualize a viable regulator in Indian environment.² I am going to be drawing by being guided by legislations that exist in countries such as: United kingdom, United state of Germany, & America. The latter are not content with any jurisdiction's current legal system. The current legal frameworks in each jurisdiction are inadequate. The Indian government passed the DPDP Act, 2023 (Digital Personal Data Protection Act) last year, which aims to strike a balance between people's rights to protect their personal data and the eventual necessity to process such data in order to fulfill legal obligations. However, the act under discussion makes no mention of artificial intelligence, such as the DPDP.

Data protection is the primary focus of the Act of 2023. Nonetheless, the EU AI Act of 2024 can be used as a model for designing Indian laws. The balance between draft and draft is important for both securing the data and information and for bolstering confidence in AI. Therefore, we will look at different jurisdictions to get an outline of the AI regulation of this article. Finding a balance between innovation and regulation is essential to promoting confidence in AI and safeguarding data and information.³ This article aims to give a general overview of AI regulation by looking at different jurisdictions, the structure needed to regulate AI, the inadequacies of the current legal and regulatory framework, the best course of action for India given its distinct socioeconomic and political environment, and the reasons why AI regulation is urgently needed globally. The paper will conclude with a summary of the entire work and a discussion of the last opinions regarding AI regulation in India.

Concept Of AI Regulation

In several sectors today, the phrase "artificial intelligence" is utilized extensively. With billions being invested in sectors like healthcare, transportation, and auto manufacturing to create AI-based solutions, it is viewed as a potential contributor to the global economy. AI is "the science and engineering of making intelligent machines, especially intelligent computer programs," according to prominent AI researcher John McCarthy. Though AI does not necessarily need to rely on physiologically observable techniques, he points out that it is related to attempts to utilize computers to comprehend human intellect. AI rules are replacing information technology regulations as the sector enters its fourth revolution.

Regulation Of AI

A collection of guidelines, practices, and trends will govern the administration of complex systems, such as artificial intelligence. In his book "Code and Other Laws of Cybercrime," activist and law professor Lawrence Lessig put forward his regulation strategy. The market, which creates economic forces; social norms, which refer to societal customs; and technology characteristics are the three main impacts he names. Governments utilize these instruments to draft certain laws. Regulations can thus take many different forms, but this study

¹ <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/#>

² <https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market>

³ K.S. Puttaswamy v. Union of India, (2014) 6 SCC 433.

concentrates on two major types. The first is stringent legislation designed to lessen adverse effects. Laws demanding adherence to AI principles or transparency norms fall under this category.

First, stringent regulations can lessen adverse effects. This includes regulations requiring adherence to AI best practices and upholding openness. Second, there exist rules that empower people and encourage creativity and efficiency. Subsidies and expedited permits for AI services and production are examples of such regulations. These general categories have been used in this research to describe AI regulation. Both kinds of rules should be coupled to improve the effectiveness and comprehensiveness of general AI regulation. The purpose of regulations on AI A balanced approach must be taken when thinking about AI legislation or policy, taking into account innovation, productivity, and safeguarding individual rights from infringement or exploitation. The goal of AI regulation is to establish a set of standards and laws to provide a secure, moral, and long-lasting environment for the advancement of society. This paper will define the purpose of AI as establishing good digital policies, unbiased AI algorithms, accountability (especially in AI development), transparency, protection against discrimination, safeguarding individual rights, and assigning responsibility (including liability). It also focuses on flexibility in frameworks, encouraging fair growth, and advancing technology. These objectives are not exhaustive. Furthermore, “for AI, trust is a must, not a nice-to-have”.⁴

AI Regulations Of Various State

The European Union: European nations are concerned about privacy and data security. The planned Artificial Intelligence Act will be put into effect by 2026, while the EU does not currently have any formal AI rules in this area. broad Purpose AI (GPAI) is defined by an update to the AI Act as systems designed by the provider to carry out broad tasks like audio and video creation or picture and speech recognition. A wide range of AI applications fall under this definition's purview. The EU is concentrating on its "EU digital single market strategy," which aims to establish guidelines for creating AI goods and services that are used inside the EU. The AI Act encourages the unrestricted cross-border flow of all AI products and services. It requires AI to be strong legally, morally, and technically, and it instructs the EU to establish a reliable system that protects basic rights and democratic ideals. Four risk categories are taken into account by the proposed law: minimum risk (AI-powered apps), high risk (such as driverless cars), restricted risk, and unacceptable risk. One important aspect of the AI Act is its risk-based methodology. The compliance of high-risk AI services and products with human monitoring is yet unknown, nevertheless. The shortcomings of the AI Act are also covered in this study.⁵ The classification of risk may provide difficulties for developers and impede the advancement of AI services and products. Since the AI Act lacks thorough definitions, it will be challenging and ambiguous to determine which goods and services fit into which categories.

United States: As of the now, AI is not subject to any particular laws or regulations. The White House Executive Order on AI addressed a number of concerns and attempted to comprehend both the hazards and the positive possibilities of AI. The "Blueprint for an AI Bill of Rights," a rights-based regulatory framework that emphasizes the necessity of AI legislation, was put out by the Biden administration and the National

⁴ Pranjal Sharma, et. al., AI Governance in India: Aspirations and Apprehension, report, Observer Research Foundation, December 6, 2023, <https://www.orfonline.org/research/ai-governance-in-india-aspirations-and-apprehensions>.

⁵ Lilian Edwards, "Regulating AI in Europe: Four Problems and Four Solutions", (2019) 1(1) *Law, Innovation and Technology* 1.

Institute of Standards and Technology (NIST). This act acts as a guide for developers or lays forth five principles. The first concept is "automated systems," which stresses data privacy, algorithms, biases, alerts, safe and efficient systems, and alternatives to human intervention. The United States hosted a closed-door meeting and a public conference in September 2023 to discuss AI rules.

China: China is keen to develop its own artificial intelligence laws that take into account new developments in technology. In May 2024, a draft rule detailing security standards for generative AI applications was released by the National Information Security Standardization Technical Committee (NISSTC). This demonstrates China's dedication to developing AI responsibly.

Sources For India: In order to maintain stringent supervision over high-risk applications and encourage innovation in lower-risk fields, the European Union has implemented a tiered approach. In the Indian setting, this risk classification method could prove advantageous. India may also learn from Singapore's emphasis on accountability, openness, and justice as well as the US AI Bill of Rights, which promotes the moral use of AI technology. China's multifaceted policy strategy also encourages cooperation between the public sector, academic institutions, and private sector. India might use Singapore's PDPA to foster responsible AI development and public confidence. Finally, the GDPR, which is presently the most successful AI policy, might serve as an example for India's regulatory initiatives.⁶

Present Conditions Of Ai Regulation In India And Prospects For The Future

Like many other countries, India perceives AI technologies as powerful opportunities and serious challenges at the same time. One of the many factors which makes India the fifth largest economy in the world, is the rapidly growing workforce. This provides an immense opportunity to attract foreign investments. There is considerable increase of foreign direct investments (FDI) in India since 2014. In 2014-15, India 45 billion in 2016-2017, reaching a peak of \$84.83 billion in 2021-2022. This trend indicates that India is likely to emerge as a major player in the Global IT ecosystem.⁷ AI projects and applications are also beginning to emerge in various sectors within the country including healthcare, business and employment. Concern regarding the privacy of data and biased AI decision making prompt Indian lawmakers to draft proposed regulations. Thus far, there is lack of enforceable laws in place, however in recent years India has aimed at developing frameworks and principles for the responsible governance of AI.

The National Institution for Transforming India, or NITI Aayog, is a key player in the formulation of AI policy in India. The National Strategy for Artificial Intelligence (#AIForAll), published by NITI Aayog in 2018, offers recommendations for advancement in a number of sectors. The establishment of AI rules in India was still being discussed in February and August of 2021.

Principles Of Operation For Responsible AI

This section discusses Responsible AI and details the consultation with non-profits, private company

⁶ **Indian Ministry of Electronics & IT (MeitY)**, *National Strategy for Artificial Intelligence #AIForAll*, NITI Aayog (2018), <https://www.niti.gov.in/strategy-national-artificial-intelligence>.

⁷ Pravin Anand, et. al., "Artificial Intelligence Law," Lexology, July 23, 2024, <https://www.lexology.com/indepth/artificial-intelligence-law/india>.

engineers, and AI developers. The goal is to apply AI in an ethical manner and develop rules according to their knowledge. Since collaboration between the public and commercial sectors as well as research institutes is essential, the government's engagement is also significant. India has formally joined the Global Partnership on Artificial Intelligence, or GPAI. In order to create laws for international standards, GPAI members endorse and encourage the implementation of the "OECD AI" principles. India still has a long way to go in terms of developing AI, though. In order to develop an AI infrastructure platform, NVIDIA Corporation has announced a collaboration with TATA Groups and Reliance Industries Ltd.

Act of 2023 for the Protection of Digital Personal Data August 9 marked the recent enactment of the Digital Personal Data Protection Act, 2023. The federal government is in the process of developing new regulations to back up the DPDP Act. When the information source is transferred by India, this legislation has extraterritorial reach and applies outside of India. According to a Boston Consulting Group assessment on AI in India, artificial intelligence is not specifically included in the DPDP Act. Nonetheless, safeguarding people's rights and private information is the act's primary objective. These databases are necessary for AI models, which rely on enormous volumes of data.⁸

Section 4 of the DPDP Act states that processing a Data Principal's personal data requires either legitimate purposes or legal permission.

In some situations, a Generative AI model may be protected by the DPDP Act's obligations when a certain data prompt is provided to it. However, the fact that such data is used to train large language models (LLMs) creates a problem. Section 6(1) of the DPDP Act, which stipulates that the Data Principal's permission must be free, explicit, informed, unconditional, and clear—that is, it must indicate an agreement to use personal data for specified purposes and only required data—is broken in this case. Additionally, Section 5 mandates that notification to the Data Principal be given in conjunction with any requests for consent under Section 6. The DSR framework (Design Science Research) is another important project under progress.⁹

To exercise rights like inspection and deletion, it is necessary to identify certain datasets that include personal information. Nevertheless, it is theoretically difficult to teach an AI model to forget the facts it has been given, and researchers are actively pursuing this objective. Neuro cloaking is a machine unlearning technique that Columbia University developers have developed, however it is extremely difficult to implement. According to this theory, AI may facilitate the application of DPDP Act rules. It is advised that AI models work on behalf of the Data Principal and function as consent managers, as specified in section 2(g), notwithstanding any potential restrictions on these models. It could be feasible to develop an AI prediction model in the future that meets consent managers' requirements.

Conclusion

The cutting-edge advancement of technology such as artificial intelligence (AI), which has the potential of being disruptive, raises ethical and regulatory, specifically legal, issues on multiple levels. The development and utilization of AI technologies in different sectors of life call for well-defined guidelines and policies on

⁸ **Varsha Bhagat-Ganguly**, "Artificial Intelligence and Law in India: Need for a Regulatory Framework", (2021) 5(2) *Indian Journal of Law and Technology* 113.

⁹ **Padmashree Sampath**, *Ethics of AI and Regulatory Challenges in India*, Observer Research Foundation (ORF), Issue Brief No. 398 (2020), <https://www.orfonline.org/research/ethics-of-ai-and-regulatory-challenges-in-india-64113/>.

them. Even though there are some ideas and new innovations in the legal framework of India, there still lacks a legal policy which focuses specifically on artificial intelligence. There is more to write in the digital law framework as The Digital Personal Data Protection Act (DPDP Act), 2023 is designed to strengthen India's position on data privacy. Though the law chiefly targets personally identifiable information, it does not deal with algorithmic transparency, system transparency, and other AI-related issues which are of equal importance. Simply put, there is a need for laws dealing with ethical use of data and AI.

Countries around the globe are now becoming one big village, sharing best practices with others on the governance of AI; the EU leads the pack with its AI Act which employs a risk-based classification framework as a means of systematically attending to AI's multilayered proliferation. Nonetheless, this could also inhibit growth and novel ideas, including fomenting ambiguity with regard to risk classification. The United States does not have a regulatory framework for AI legislation, but makes some effort to address bias and accountability issues with its "Blueprint for an AI Bill of Rights." Regulation in China.

India requires a comprehensive approach that fosters creativity alongside strong safeguards for privacy and personal data. With respect to the country's IT sector, foreign investments, and AI adoption, there is promising growth potential. Programs like NITI Aayog as well as the country's participation in GPAI gives India the opportunity to build a tailored regulatory system that takes into account local needs and global standards. Striking the balance between public interest and allowing innovation with responsibility needs to become the focus of legislation in order to encourage ethical AI development in the country. If successful, India can emerge as a leader in the responsible evolution and governance of AI technology, establishing a balanced system that nurtures innovation while upholding fundamental rights.

References

1. <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/#>
2. <https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market>
3. K.S. Puttaswamy v. Union of India, (2014) 6 SCC 433.
4. Pranjal Sharma, et. al., AI Governance in India: Aspirations and Apprehension, report, Observer Research Foundation, December 6, 2023, <https://www.orfonline.org/research/ai-governance-in-india-aspirations-and-apprehensions>.
5. Lilian Edwards, "Regulating AI in Europe: Four Problems and Four Solutions", (2019) 1(1) Law, Innovation and Technology 1.
6. Indian Ministry of Electronics & IT (MeitY), National Strategy for Artificial Intelligence #AIForAll, NITI Aayog (2018), <https://www.niti.gov.in/strategy-national-artificial-intelligence>.
7. Pravin Anand, et. al., "Artificial Intelligence Law," Lexology, July 23, 2024, <https://www.lexology.com/indepth/artificial-intelligence-law/india>.
8. Varsha Bhagat-Ganguly, "Artificial Intelligence and Law in India: Need for a Regulatory Framework", (2021) 5(2) Indian Journal of Law and Technology 113.
9. Padmashree Sampath, Ethics of AI and Regulatory Challenges in India, Observer Research Foundation (ORF), Issue Brief No. 398 (2020), <https://www.orfonline.org/research/ethics-of-ai-and-regulatory-challenges-in-india-64113/>.