
POLICY FOR THE FUTURE: AI POLICY DRAFT

SAMBIT ACHARYA | B.A. (H) POLITICAL SCIENCE 3RD YEAR | DESHBANDHU COLLEGE

Email Id - sambit.acharya2004@gmail.com

INTRODUCTION

Since the advent of Artificial Intelligence in mainstream multimedia on the World Wide Web, both novel uses and fears about the technology have resurfaced amidst the way it has radically changed how we surf the web. Right as the world was reeling with the Covid-19 Pandemic, a quiet revolution took place in the form of Artificial Intelligence for the general public in Silicon Valley. This new wave of technology was thus born.

Even though Artificial Intelligence has existed as tidbits throughout the 2010s, it was only ever used to power algorithms for popular social media sites such as YouTube, or used in complex calculations in scientific research. It was not until 2022 Q2 that the world was introduced to “ChatGPT”, the GPT standing for “Generative Pre-trained Transformer”, which refers to a Large Language Model that is trained on datasets and is capable of “transforming” text into numerical notations for the model to create new content. Unlike human language, the natural language such as AI models understand by comparing and conjoining nodes that may contain words, phrases, sentences and numerals. Artificial Intelligence is mostly used in repetitive, redundant tasks deemed to be unproductive for humans. Generative AI, known as “GenAI” in short, is a form of AI that is used to generate text, images, videos and other forms of data consumables. But as is true for every single revolution in the world, this too has had its fair share of consequences to go along with the supposed

positive impact. Some of them may include misuse of digital identity, increase in cyberattacks such as phishing and bruteforcing techniques, unauthorized access to files and accounts, non-consensual creation of deepfakes and generative personas infringing upon identity rights of a person, and so on. This is why there must be an urgent need to draft a public policy regarding the usage, administration and moderation of AI in India.

This draft policy aims to act as a suggestion for a formal AI policy that should govern the usage, administration and data access for AI companies while respecting the IT Act, 2000 and the DPDP Act, 2023 and DPDP Rules, 2025. Data sovereignty is the key in this policy as we are witnessing rampant violation of the same due to lack of stringent AI policies in the country. This draft will bring a meaningful background from a policy-based perspective, followed by the scope of the draft policy in terms of effectiveness, application and efficiency. This shall be followed by a brief evaluation of former, broader policies where efforts have been made to address basic AI policies. Following this would be a detailed draft policy for AI, consisting of steps for formulation and implementation of the same. Probable outcomes and possible immediate implications shall also be assessed, given the rapidly-changing world of Information Technology. At the end, future prospects for further policies shall be discussed upon.

BACKGROUND

(A.) IT ACT, 2000



The IT Act of 2000 was the first major step taken up to ensure regulation and administration of Information Technology in the backdrop of the IT Sector boom in India between 1990-2000. It addresses various laws such as copyright, handling of personal information, intellectual property and patents, alongside the expansion of fundamental rights in cyberspace. It also defined multiple provisions to address data safety, violation of rights, cyber offences as well as issuance for blocking content deemed harmful for public access. The Act went through two major amendments, the IT (Amendment) Act, 2008 and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, respectively. Together, these amendments aimed at greater accountability on the part of individuals, intermediaries and companies, while simultaneously prioritising internal digital safety as a mandatory measure. But these were never designed while keeping in mind the development of Artificial Intelligence, being drafted at a time when AI was still a dream of the near future. Its data protection provisions were meant to prevent regular corporate negligence while handling sensitive data of Indian users, but were fundamentally ill-equipped to handle algorithmic processing and synthetic content generation.

The Act does not have a sufficient framework to handle AI based accountability systems and transparency, resulting in the judicial system to interpret violations in the domain of personal rights, privacy and identity-theft as creatively as possible.

(B.) DPDP ACT, 2023 AND DPDP RULES, 2025

The Digital Personal Data Protection Act, 2023 aimed to enhance the applicability of the IT Act, 2000, to be applicable to a much larger domain in terms of the Internet and distinct concepts in the domain of ICT. This Act establishes distinct stakeholders that act as policy actors and form the backbone of the ICT industry in India. Examples include Data Principals, Data Fiduciaries, Data Protection Board, to name a few. It puts greater accountability on companies to adhere to the Right to Privacy of Indian citizens, which is to be carefully scrutinized at every point where technology is used. It does, however, exempt the government itself from scrutiny, as well as raising suspicion with the mechanism of direct appointments to the Data Protection Board by the Central Government, followed by the removal of Journalistic Exemptions, which massively impacts Press Freedom in India. There is also a clear lack of provisions governing AI usage and specific rules meant for Significant Data Fiduciaries (SDFs) dealing with AI products in India. The Digital Personal Data Protection Rules, 2025, much like the IT Rules, 2021, are meant to serve as the implemented step for the DPDP Act, 2023. It suggests a phased implementation for Fiduciaries to adhere to the rules accordingly with transitional urgency in place. This would be embracing a “digital-by-design” philosophy, suggesting a transition from physical offices to fully-online portals and sites for grievances and management of Digital Personal Data.

It is intended to provide greater and direct access to Data Principals across the country. Much like the DPDP Act, the DPDP Rules have limited or vague applicability limits when it comes to AI usage and AI administration in India, which can invite major risks in avenues such as automated decision-making without human intervention, algorithmic bias and liability of harm done by AI, to name a few. Therefore, a dedicated AI Policy is the need of the hour for India. If we talk about recent judgments in the sphere of AI, we can include *Anil Kapoor vs. Simple Life India & Others.* and *Rajat Sharma vs. Union of India* cases, where petitions were filed regarding the regulation of deepfakes while addressing breach of consent of the persons involved in misuse of identity. We can also talk about *Arijit Singh vs. Codible Ventures LLP* and *Shilpa Shetty vs. Getoutlive.in & Others.* cases to understand how AI can be misused to synthesize content based on the person's likeness, voice and face to harm the person as well as defraud unsuspecting victims.

SCOPE

The scope of this supposed AI policy needs to be as big as the DPDP Act, 2023 and the DPDP Rules, 2025, as it is an essential extension of the same, while also having carefully crafted minute provisions that cater to the needs at the local level and at organisational levels where AI is required for increase in productivity in terms of assistance and efficiency of work. It should bear in mind the same fundamental and individual rights enjoyed by Indians as per the IT Act, 2000, without which, it might virtually degrade over time in terms of effectiveness. The Policy must cover stakeholders on a local, state and central level to better serve the requirements of the Data Principals with relative context to back it all up. There should also be a dedicated organization for filing of

E-grievances related to AI and its use/misuse by/against the complainant. Overall, the goal must not be to alienate AI completely, but rather, to embrace it with necessary safeguards to ensure overriding of the policy by a third actor without any consequences.

FORMULATION

The policy formulation should undertake the following crucial steps as its fundamental basis:-

- The policy must begin with stakeholder meetings, which include but are not limited to: Minister of Electronics and Information Technology, CEOs of AI SDFs, domain experts dealing in AI, founders/directors of civil societies such as NGOs championing Individual Rights of Privacy and Freedom of Expression, Specific Parliamentary Committees, with extensive services provided by Civil Servants with a technical background or expertise in terms of ICT. Together, with more weightage given to civil societies and public opinions raised on sanctioned forums, the policy should have a multi-pronged stakeholder management system to avoid overriding of crucial mechanisms,
- Investment into AI and Cybersecurity must be done to ensure minimal breaches at every step, while adhering to the IT Act, DPDP Act and Rules, and fulfilling the principles of the Digital India Mission. Cybersecurity is often the culprit behind non-AI driven data breaches, so it's important to have a dedicated mini-cybersecurity policy in place.
- An AI Commission should be convened under the MeITY, where stakeholders can act as members with equitable decision-making powers. This can keep the AI Policy well-organized, and accountable with relative ease of access
- Development of in-house resources in AI technology should be encouraged under the

Atmanirbhar Bharat mission for enhancing data sovereignty of the AI data generated by Indian users. For example: SarvamAI, KrutrimAI, Khoj.

- Analysis of potential conflicts arising out of similar but incomplete provisions of other related policies, and enabling a conflict resolution management system to ensure checks and balances cannot be used against any other part of the Policy.

IMPLEMENTATION

As far as implementation of the AI policy is concerned, we must look at the responsibilities and enforcement mechanisms to be addressed. The responsibilities for each stakeholder should broadly be arranged as follows:-

Companies:

Data Fiduciaries and Significant Data Fiduciaries dealing with AI, especially DFs from overseas, must adhere to AI Retention policies, where, unless requested by the Indian user, data must be maintained in servers on Indian soil. Criminal investigations, however, override user consent in data retention choices, which shall include all citizens of India and Non-Residential Indians. AI misuse reporting mechanisms must be strengthened, with efficient responses to complaints about breach of consent and/or data. Mandatory internal auditing every 4-6 months ensuring best practices for Indian AI policies are followed at all times. Elimination of Dark Patterns in any AI product to prevent unaccounted data breaches.

Government:

Appointment of Consent Managers to coordinate with Fiduciary-appointed Point of Contact to enable quick redressal of user requests and government requests at the same time. PSAs meant to educate the general public in handling AI with care, and showing best practices to safeguard personal data.

Appointment of a special fact-checking body (inspiration from PIB Fact Check can be a good start), specifically meant to distinguish and discourage AI usage in spreading of misinformation, with efficient checks and balance to ensure minimal damage.

Civil Societies:

Convening of weekly meetings with other stakeholders to ensure consistent transparency and accountability.

Local-level AI Panchayats to provide hands-on training on handling AI at the local and district level. Organisation of awareness campaigns for effective prevention from common scams and fraudulent acts associated with AI misuse.

General Public:

Enhancement of public discourse by personal research, discussion in relevant forums and events. Cooperation with other stakeholders and public authorities if in case of a criminal proceeding. Speedy digital trials with physically-traceable evidence to minimize faulty petitions. Enhancing ease of access to AI to peers and family with reasonable guidance on AI policy and AI usage guidelines. Prompt reporting of instances of AI misuse to the Data Fiduciary/Consent Manager/Point of Contact.

To enable effective enforcement of the policy, following may be considered as a good baseline:-

- *Compliance guidelines:* A flexible, incremental penalty system to place monetary constraints on mishandling of AI administration by Data Fiduciaries, followed by a strict framework for authorities to take action against repeat offenders. Company policy should reflect compliance with the AI Policy.
- *Terms of Termination:* A clear document highlighting terms of termination of Data Principals, Data Fiduciaries and Consent Managers upon violation of Right to Privacy and data breaches.

- *Periodic Auditing:* Documentation clearly mentioned in the Terms of Service of Data Fiduciaries for mandatory periodic auditing by third-party auditing bodies. Frequency can be between 4-6 months.
- *Mandatory temporary consent mechanism:* Data Principals are required to be asked about their consent to provide their data to AI companies within a period of once every 3-4 months.
- *Ethical reviews:* Data Fiduciaries may be advised to organize ethical reviews of AI models from time to time in order to prevent potential harm with AI, mentally and/or physically.

When it comes to constant development and flexible administration of AI, domain experts can be invited as advisors to guide the government on the development and administration of AI, along with periodic assessment of new technologies in the sphere of AI, while holding parallel discussions in transparent forums for AI in India. Domain experts can also play a significant role in settling legal issues pertaining to AI in the judicial system.

IMPLICATIONS, OUTCOMES AND FUTURE PROSPECTS

Assuming this is a complete policy for AI administration and management in India, it will have deep implications in the development of AI, in the wake of massive investments being done by “Big Tech” companies such as Nvidia and Google in development of AI Data Centres and incentives for Indian users. Now is the perfect time to utilize the somewhat vague terms of the DPDP Rules, 2025 and expand it forward, starting with AI and subsequently to other related fields within the domain of ICT. Some immediate outcomes may include greater public awareness for data safety, with public discourses already being held on the same as the perfect platform to shape an inclusive model for AI governance. Further implications may include a truly sovereign, efficient and working model to prevent unauthorized access to Data Principals’ data without explicit consent, which is still in a grey area when it comes to usage of AI and other technological products. It can also serve as the basis for other tech companies entering the Indian market to enter into an equitable transaction of complying with local AI laws while wanting to gain profit margins in a big market such as India. This draft policy is meant more as a set of basic suggestions and directives to get started with a truly effective AI Policy that shall govern it within Indian territory. Therefore, it has a lot of scope to be inspired from AI policies being followed around the world, and ensure the parts which are fair and democratic in nature to be deemed fit for an Indian adaption accordingly. Such a comprehensive AI policy that acts out in a similar fashion as our Constitution in a well-codified manner will help other world governments to be inspired and ensure a sustainable and healthy manner of AI administration that enshrines the value of democracy, peace and cosmopolitanism

REFERENCES

- Government of India, Ministry of Information Technology. (2000). The Information Technology Act, 2000 (Act No. 21 of 2000). Ministry of Electronics and Information Technology. https://www.meity.gov.in/static/uploads/2024/03/IT-Act-Rules_2000_0.pdf

- Government of India, Ministry of Law and Justice, Legislative Department. (2023, August 11). The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Gazette of India Extraordinary, Part II, Section 1. <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>
- Ministry of Electronics and Information Technology, Government of India. (2025, November 17). DPDP Rules, 2025 notified: A citizen-centric framework for privacy protection and responsible data use. Press Information Bureau. <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf>
- Kapoor, A. v. Simply Life India & Ors., CS(COMM) 652/2023 (Delhi High Court, September 20, 2023). Indian Kanoon. <https://indiankanoon.org/doc/113724486/>
- Rajat Sharma & Anr. v. Ravindra Kumar Choudhary, CS(COMM) 456/2024 (Delhi High Court May 30, 2024). <https://www.scconline.com/blog/post/2024/06/11/delhi-high-court-restrains-baap-ki-adalat-for-infringement-rajat-sharma-aap-ki-adalat-show-legal-news/>
- Singh, A. v. Codible Ventures LLP & Ors., COM IPR Suit (L) No. 23443 of 2024 (High Court of Bombay, July 26, 2024). LiveLaw. https://www.livelaw.in/pdf_upload/arijit-singh-vs-codible-ventures-llp-552701.pdf
- Kundra, S. S. v. Getoutlive.in & Ors., Interim Application (L) No. 38469 of 2025 in Commercial IP Suit (ST) No. 38338 of 2025 (High Court of Bombay, December 26, 2025). Courtbook. <https://s3.courtbook.in/2025/12/Shilpa-Shetty-Kundra.pdf>