The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

Unlocking the Future: Is the Latest Digital Personal Data Protection Act Prepared for the AI Revolution?

INTRODUCTION

Privacy is a right linked to one's person. It is a way of exercising one's will, and how one wants to lead their life. It is in a wide connotation, a choice and liberty to make decisions for oneself. Personal liberty and privacy are synonymous in several contexts. Often, they are considered two sides of the same coin. In 2017, after much deliberation, the right to privacy was recognised as a fundamental right under Article 21 of the Indian constitution. *Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors*., one of the landmark judgements in the history of the Indian judiciary, laid down a framework for privacy rights in India. In the present atmosphere, informational privacy, a facet of the right to privacy[1], has become a hot topic for discussion, more so after the enactment of the Digital Personal Data Protection Act, of 2023 (DPDP). As we are transitioning, from a world run by 'Google' to a world accelerated by 'ChatGPT', the probability of getting exposed to a data privacy breach has increased exponentially. Data Privacy is one of the facets of informational privacy and is related to the protection of one's identity[2]. Data is a wide pool of information related to a particular thing(s). Any data about an individual who is identifiable by or in relation to such data is known as 'Personal Data'[3]. Artificial Intelligence (AI) based tools extensively process such personal data and are fed on this data to function. This calls for a state-wide regulation to monitor such activities, ensuring a delicate balance between protecting individuals' rights and facilitating the legitimate processing of personal data.

DPDP ACT AND AI

The recently promulgated DPDP Act endeavours to address the needs of both data fiduciaries and data principals. The legislation's effectiveness will be rigorously scrutinized upon enactment, especially with AI's growing influence on the internet landscape. As AI continues to evolve and exert its influence, the extent to which the DPDP Act effectively safeguards

[1] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.
[2] Ibid
[3] Digital Personal Data Protection Act, 2023

personal data and maintains a balance between the users and the providers will be thoroughly scrutinized. The act has laid down certain pre-requisites before processing any personal data-

- It should be for a lawful purpose
- Consent of the data principal is a must
- Consent of the data principal may not be required in case data processing is for a legitimate use

Lawful purpose means any purpose not expressly forbidden by law[4]. There is no definition or clarification provided for the term 'legitimate use', leaving room for uncertainty and misuse. Referring to the EU's regulation on this aspect, the General Data Protection Regulation (GDPR) has included several illustrations, and through its recitals and policy directives that led to the formation of the regulation, it offers more perspicuity.

While these provisions in the DPDP Act offer a broad overview of the responsibilities of a data fiduciary regarding consent and legitimate use of data, more nuanced, specific, and detailed provisions are needed to tackle the complex challenges posed by AI-driven software in processing personal data.

ADDRESSING AI BIAS CONCERNS

An AI-driven tool is trained on gargantuan data that is available online and is likely to inherit the biases. "*AI bias occurs because human beings choose the data that algorithms use, and also decide how the results of those algorithms will be applied. Without extensive testing and diverse teams, it is easy for unconscious biases to enter machine learning models. Then AI systems automate and perpetuate those biased models".* So, while the data may be collected with the consent of the data principal, it may perpetuate discrimination or introduce bias inherited within the algorithm. This bias can originate during data collection or manifest later, depending on the circumstances. A similar concern was shown in the Puttaswamy judgement, "*Another aspect which data protection regimes seek to safeguard is the principle of non-discrimination which ensures that the collection of data should be carried out in a manner which does not discriminate on the basis of racial or ethnic origin, political or religious beliefs, genetic or health status or sexual orientation.*"[5] The primary goal is to safeguard data principals from biases, whether during collection or processing stages

The present act does not address this problem and is the only legislation in existence that deals with data processing online. This is a problem that requires urgent attention from the stakeholders. Data Robot's State of AI Bias report reveals that 81% of the technology leaders want government regulation on AI bias.[6] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code), has laid down certain rules that briefly address

[4] Ibid, section 4

[5] Supra note 1, at para 178

[6] Rogers, S. (2023) Datarobot's State of Ai Bias Report reveals 81% of technology leaders want government regulation of Ai Bias, DataRobot AI Platform. Available at: https://www.datarobot.com/newsroom/press/datarobots-state-of-ai-bias-report-reveals-81-of-technology-leaders-want-government-regulation-of-ai-bias/ (Accessed: 09 April 2024).

this issue and the advisory issued by the MEITY on 15th March 2024 has reiterated the need to evaluate the automated tools concerning 'the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools'[7]. The advisory issued states that the AI models should not promulgate bias or discrimination or threaten the integrity of the electoral process. It does not specify any liability or responsibility of developers in case of a violation. However, it iterates that non-compliance with IT Rules will lead to penal consequences.

CONCLUSION

The existing law in India is not sufficient to address the problems presented by AI and requires more specific provisions directly dealing with this predicament. While laws, including the forthcoming DPDP Act and the implemented Information Technology Rules, demonstrate some acknowledgement of the challenges posed by AI but fall short of providing comprehensive solutions. As AI continues to shape our digital landscape, a dedicated law is essential to effectively mitigate issues posed by AI, uphold privacy rights, and foster trust in AI technologies. It is time for policymakers to prioritize the enactment of legislation specifically tailored to address the complexities of AI bias and discrimination.

[7] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.