NAVIGATING THE REGULATORY LANDSCAPE FOR AI AND PUBLICLY AVAILABLE DATA IN INDIA

Ishnay Prakash & Dhruv Sanjeev Purkar, School of Law, CHRIST (Deemed to be University), Bengaluru

ABSTRACT

Artificial Intelligence stands at its potential zenith today as it is rapidly evolving and giving way to fast technology. As AI is made to deal and delve into data in order to make it function, the access to publicly available data and its interaction with AI gives rise to a set of legal intricacies. This legal research paper delves into the complex and evolving regulatory framework governing the intersection of Artificial Intelligence (AI) and publicly available data in India. The paper meticulously navigates the changing regulatory landscape within India, placing specific emphasis on the contentious Section 3(c)(ii) of the Digital Personal Data Protection Act, 2023. This clause, which extends exemptions to publicly available data, beckons a close examination due to its far-reaching implications. This paper encapsulates a comprehensive legal exploration into the consequences of Section 3(c)(ii) concerning the processing of individuals' personal information for AI applications. The paper analyzes various legal provisions in the present machinery of AI and Data Protection framework and viewpoints of the Hon'ble Supreme Court. It further goes on to suggest the imperative need for a well-balanced legal and policy framework, which, while facilitating AI innovation, steadfastly safeguards the fundamental rights to privacy within India's evolving data protection laws.

Introduction

The Right to Privacy has seen a rapid transition from the Supreme Court denying it[1] to accept it and further recognize it as a fundamental right[2]. India stands at a critical juncture in the dynamic intersection of Artificial Intelligence (AI) and data privacy. In an era characterized by rapid advancements in Artificial Intelligence (AI)[3] and the increasing ubiquity of data, the regulatory framework governing the interplay between AI and data privacy has emerged as a pressing concern globally and within the Indian context. India, a burgeoning technology hub, finds itself at the nexus of innovation and data protection, poised to navigate the intricate landscape where these two domains intersect. The evolving regulatory landscape of data protection in India has witnessed significant developments driven by the need to align with global privacy standards, address emerging challenges, and safeguard individuals' fundamental right to privacy. Building upon the foundation laid by the Information Technology Act, 2000 (IT Act), recent legal advancements, including the landmark judgment of the Supreme Court in ***Puttaswamy***[4], and the proposed Data Protection and Privacy Bill (DPDP Bill), mark a transformative phase in India's approach to data protection.

Through this paper, the authors are contending that Section 3(c)(ii) of the Digital Personal Data Protection Act, 2023 is capable of being abused or overused. It further explores the potential legal and policy implementations of the clause in question in the context of rigorous growth and application of AI. The paper relies on various laws and bills previously enacted and debated upon. It uses doctrinal methodology of research, within which a grounded method was used to analyze laws, rules and the judgments of the Hon'ble Supreme Court, relevant in this field. The aspect of privacy and safeguarding of data is viewed through various lenses that have come up as a result of numerous interpretations of the Apex Court with significant reliance on the Puttaswamy Judgment. The literature reviewed involve other judicial precedents and bills previously brought forth by the legislature.

Foundational Framework: The Information Technology Act, 2000:

The IT Act, enacted in 2000, served as India's initial response to the challenges posed by the

[1] *Kharak Singh v. State of UP,* 1963 AIR 1295
[2] *Retd. Justice K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1
[3] AI and Interpreters; https://qinterpreter.com/2023/08/, last accessed March 9, 2024 at 7:15 P.M.
[4] *Retd. Justice K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1

digital era.[5] The objective of the act was to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce"[6], which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.[7]

While it laid the interim foundation for regulating electronic transactions and digital signatures, its provisions about data protection were limited in scope and needed more depth to address contemporary privacy concerns. The authors thereby contend humbly that the Act should have comprehensively addressed issues such as data breaches, cross-border data transfers, or the rights of data subjects. It is also contended that these issues are raging wide in the contemporary world and have to be addressed with a strong hand.

Recognition of Privacy as a Fundamental Right through the lens of Retd. Justice K.S. Puttaswamy v. Union of India[8]

The Indian Constitution guarantees to all of its citizens the fundamental right to life.[9] Justice K.S. Puttaswamy (Retd.), a retired judge of the Madras High Court, challenged the constitutional validity of the Aadhaar scheme. He argued that the scheme violated the right to privacy. A three-judge bench held that a larger bench should determine whether the Constitution of India guarantees a right to privacy. The matter was therefore referred to a 9 Judge Bench of the Supreme Court to dive deeper into the privacy issue. The issue before the bench was regarding the issue of Privacy and whether the same should be a recognized right or not.

The Hon'ble court recognized the right to privacy as a fundamental right intrinsic to the right to life and personal liberty under Article 21 of the Indian Constitution.[10] This right encompasses the protection of an individual's autonomy, personal space, and dignity against unwarranted

[5] Is India lacking in securing its citizens' privacy in this digital era?; https://timesofindia.indiatimes.com/blogs/polymathwriter/is-india-lacking-in-securing-its-citizens-privacy-in-this-digital-era/; last visited April 1, 2024 at 7:30 P.M.
[6] Preamble to the Information Technology Act (21 of 2000)
[7] *ibid.*
[8] (2017) 10 SCC 1
[9] Article 21, Constitution of India, 1950
[10] *ibid.*

intrusions. The judicial landscape shifted dramatically with this Supreme Court's judgment. Being extremely pivotal, the judgment laid the foundation for developing a more robust and comprehensive data protection regime in India, acknowledging the evolving challenges posed by the digital age. The court affirmed that privacy is crucial for the exercise of other rights and freedoms, emphasizing its status as an essential element for the meaningful enjoyment of life and liberty. The evolution of privacy laws is a complex and multifaceted journey that spans centuries and has been shaped by societal, technological, and legal developments.[11]

The judiciary, not just in the abovementioned judgment has evolved and conceptualized the Right to Privacy via its wide interpretations. In the context of privacy, individuals have the right to control their personal information, decide who can access it, and determine the purposes for which it can be utilized. The concept extends beyond physical spaces to include informational privacy, protecting individuals from unwarranted surveillance, data collection, and dissemination. The apex court, in ***R. Rajagopal judgment***[12], recognized the right to privacy as an inherent part of personal liberty. The court held that an individual's right to privacy must be respected, and the publication of private, non-public facts without consent could be an invasion of privacy. The concept of privacy, as a fundamental right, has evolved along with inclusion of privacy laws as enacted by the legislature in lieu of these judgments of the Court. Let's understand the history of India's data privacy law landscape.

The Personal Data Protection Bill, 2019

In December 2019, India introduced the Personal Data Protection Bill ("PDPB 2019"), following the example of many other significant data privacy laws being introduced worldwide. PDPB 2019 aimed to reform India's legal system and establish standards for cross-border data transfers, the accountability of entities processing personal data, and remedies for unauthorized and harmful personal data processing. The bill faced significant criticisms, especially regarding the regulation of social media platforms and requirements of data localisation, which raised concerns for potential violation of fundamental rights of the citizens of India and being non-friendly for businesses and platforms to operate in India.[13]

[11] The Evolution of Privacy: A Look at the Past, Present and Future; https://www.cga.ct.gov/PS98/rpt%5Colr%5Chtm/98-R-1455.htm, last accessed March 18, 2024 at 5:40 P.M.
[12] *R. Rajagopal v. State of Tamil Nadu*, 1995 AIR 264
[13] An Analysis of the Personal Data Protection Bill, https://www.livelaw.in/articles/an-analysis-of-the-digital-personal-data-protection-bill-231161, last accessed April 2, 2024 at 5:45 P.M.

Way Further: Data Protection Bill 2021 & 2022

Data Protection Bill 2021 ("DPB 2021") made key revisions to the previous bill. This included adding personal and non-personal data and imposing strict guidelines for reporting data breaches. DPB 2021 was thought to be passed and become an official part of India's legislature as the Data Protection Act 2021. However, the bill was withdrawn altogether in August 2022 by the Indian government - after three years of discussion and 90 sittings - because it failed to meet international standards and upcoming challenges. After the much-awaited 2021 bill was withdrawn, all eyes have been on the Indian government and Parliament for an update on the new bill.

Digital Personal Data Protection Act 2023

After much deliberation, the updated version of DPDP 2022 was tweaked, and the new version of the Bill, i.e. DPDP Act 2023, was presented in the Indian Parliament on 3rd August 2023. It was passed by the Parliament on 9th August and gazetted on 12th August 2023, officially becoming the DPDP Act. The DPDP Act's objective is to provide standards for handling digital personal data in a way that respects both people's rights to privacy protection and the need to handle personal data legally. It outlines the duty of data fiduciaries (data handlers/controllers), the rights of the principals (data subjects), and the consequences of non-compliance. India's digital economy is booming, fueled by an increasingly data-driven landscape. This growth, however, has been accompanied by concerns surrounding the collection, storage, and use of personal data. In response, the Indian government introduced the Digital Personal Data Protection Bill, 2022 (DPDP Bill) (Government of India, 2022),

The Act provides for the processing of digital personal data in a manner that recognizes both the rights of the individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.[14]

The Act protects digital personal data (that is, the data by which a person may be identified) by providing for the following:

- The obligations of Data Fiduciaries (that is, persons, companies and government

[14]Salient Protection of the Digital Personal Data Protection Bill, 2023; https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264; last accessed March 22, 2024 at 12;10 P.M.

entities who process data) for data processing (that is, collection, storage or any other operation on personal data);

- The rights and duties of Data Principals (that is, the person to whom the data relates) ;and
- Financial penalties for breach of rights, duties and obligations.

The major and the key highlights of the act are:

1. **Applicability**: Applicable to processing digital personal data within India (online or offline, digitized) and outside India only when profiling or offering goods/services to individuals within India.
2. Lawful purpose and informed consent.
3. Data minimisation and storage limitations.
4. Data Principal Rights: Grants individuals various rights, including:
5. Right to information about data processing.
6. Right to access and rectify data.
7. Right to restrict or erase data.
8. Right to data portability.
9. Data security measures.
10. Cross-border data transfer restrictions.
11. Data Protection Authority: Establishes a Data Protection Authority of India for regulatory oversight, grievance redressal, and enforcement.

Disputed Provision of the Act: Section 3(c)(ii) & its Analysis

The author has based this research regarding the mentioned clause of the DPDP Act, 2023.

Section 3(c)(ii) exempts certain publicly available data from the application of this act. Some provisions, like data localisation requirements, apply only to entities processing the data of a certain number of individuals, potentially creating loopholes for smaller entities. While the Act aims to empower individuals with control over their personal data, its provisions have sparked debate, particularly Section 3(c)(ii) which grants unfettered access to publicly available personal data under certain circumstances. This paper meticulously navigates the evolving regulatory landscape in India, placing specific emphasis on the contentious Section 3(c)(ii) and its implications for individual privacy and data security.

Introduced to establish a concrete data protection regime, the Act aligns with international standards like the Global Data Protection Regulations, yet tailors its provisions to meet India's specific socio-economic conditions. Section 3(c)(ii), in particular, determines as to where the provisions of this Act would not apply. It states that any publicly available data either by the owner of the data or the Data Principal, is not within the purview of this Act. This clause is important in balancing interests of the intermediaries or data middlemen with individual data rights, though the data being publicly available. Section 3(c)(ii) has sparked debate due to its broad language, which could potentially be exploited to bypass consent requirements under the guise of legislative functions. Critics argue that this may lead to overreach by the present application of AI in various sectors of the industry by various stakeholders, at multiple facets, thereby diluting the privacy safeguards the Act aims to establish.[15] Ethical deployment of AI technologies, particularly in sensitive sectors like healthcare and law enforcement, becomes disputable as AI is implemented quite often to work upon publicly available data, the application of which would not be scrutinized by law as per the exemption given by Section 3(c)(ii).[16] The implementation of Section 3(c)(ii) raises intricate overuse issues, particularly regarding the scope of "necessary" data processing activities by the intermediaries thriving with the usage of AI. The lack of a stringent oversight mechanism or clear limits could lead to privacy erosions, undermining the trust in India's digital economy.[17] The author contends and humbly submits that there needs to be a robust ethical framework to ensure that AI applications

[15] 15 Major Problems with India's Digital Data Protection Bill, 2023; https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023/, last accessed March 22, 2024 at 5:50 P.M.

[16] Marda, V., 2018. Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376; https://doi.org/10.1098/rsta.2018.0087

[17] Viljanen, M., & Parviainen, H. (2022); AI Applications and Regulation: Mapping the Regulatory Strata. Frontiers in Computer Science; https://consensus.app/papers/applications-regulation-mapping-regulatory-strata-v

respect data protection principles and individual rights, despite being available in the mainstream. To provide an instance, a patient's report that has to be proofread and audited by the reporter is often publicly visible. The application of AI to work with such data raises concerns regarding its overuse by the fiduciary deploying the AI to use. Any usage of such data that is public, beyond its authorized limit, shall constitute an overuse and a violation of the rights of the data holder. Such an overuse is not protected under the DPDP Act by virtue of Section 3(c)(ii). When such data is processed by AI , it has the potential to be misused and such data becomes vulnerable to abuse. The authors have understood and considered this to be a major concern which can potentially arise in the forthcoming period and there is a need felt to address the same. It is quite the possibility that AI can be overused either intentionally or due to an error via syntax or run-time that such data can be exploited. The authors are therefore suggesting recommendations which can be useful to tackle such an issue and regulate it.

Recommendations and Conclusion

Based on the research and analysis carried out above, the author has come down to a few suggestions regarding the research problem. These are humble recommendations to aim to address the shortcomings of the existing regulatory frameworks and enhance the robustness of AI governance. To address the challenges posed by Section 3(c)(ii), this paper recommends the establishment of clearer guidelines defining the scope of necessary functions that justify data processing that is available to the world at large. Additionally, enhancing transparency and accountability measures for AI applications can mitigate potential abuses and foster public trust. Section 3(c)(ii) of the Digital Personal Data Protection Act, 2023, represents a critical intersection of legislative function and privacy rights. While it aims to facilitate governmental operations, its broad application could pose significant challenges to privacy protection in India. As such, it is imperative that this clause be implemented with stringent safeguards to prevent misuse and ensure that India's digital governance framework remains both effective and respectful of individual rights.

The authors feel that there is a pressing need for comprehensive ethical guidelines that dictate the development and deployment of AI technologies. These guidelines can be aimed at addressing critical issues such as bias mitigation, transparency, accountability, and the impact of AI on privacy and human rights, and how such guidelines govern the interaction facilitating between AI and publicly available data. The central AI regulatory authority, in collaboration

with industry stakeholders, can be tasked with the development and enforcement of these guidelines. Given the rapid pace of technological advancements in AI, it is imperative that AI regulations are not static but dynamically adapted to new challenges and innovations. Regular reviews of the regulatory frameworks should be mandated, with provisions for timely updates to address emerging issues and integrate technological advancements. The regulation of AI and the governance of publicly accessible data within India are at a pivotal crossroads. The swift advancement of AI technologies has created a pressing requirement for a legal framework that is proactive and flexible. In addition to addressing the current issues, such a framework needs to foresee future technology developments in a proactive manner. It should make sure that the advantages of AI are optimized while also defending people's rights and social standards. By adopting these recommendations, the current status can position itself to potentially lead in the realm of ethical AI development in consonance with privacy. It is believed that changes incorporated will further attempt to safeguard the overuse of data caused by AI of publicly available data.