Convergence of Artificial Intelligence and Privacy Rights in India's Legal Framework

Ashish Kumar Singh

Assistant Professor, Law, S.K.J Law College

Abstract

The rapid advancement of Artificial Intelligence (AI) poses significant challenges to the right to privacy, particularly in a legal context like India's . As AI systems increasingly integrate into various aspects of life—ranging from healthcare to law enforcement—the potential for privacy infringements grows. Personal data, often at the heart of AI operations, is vulnerable to misuse, raising concerns about surveillance, data breaches , and the erosion of individual privacy . India, with its emerging data protection laws and constitutional recognition of privacy as a fundamental right, is navigating this complex landscape . The legal framework must balance AI's potential benefits with robust privacy safeguards to protect citizens' rights.

Keywords: Artificial Intelligence, Privacy, Data Protection.

1. Introduction

India currently lacks a fully developed data protection law, though the Digital Personal Data Protection (DPDP) Act of 2023 was recently enacted . The Act seeks to regulate the handling of personal data, introducing safeguards like data localization and consent requirements . However, there are ongoing concerns regarding possible exemptions for government bodies and whether the legislation adequately addresses AI-specific challenges. The Indian judiciary has also stressed the importance of balancing privacy with interests such as national security, crime prevention, and social welfare . The Supreme Court's landmark Puttaswamy case recognized privacy as a fundamental right, while also affirming that it is not absolute .

As AI continues to be integrated into various sectors, policymakers must be mindful of the privacy implications . A comprehensive governance framework, ethical standards, and regulatory oversight are essential to ensure that AI development respects constitutional rights and democratic values . Achieving a balance between innovation and privacy protection is key to fostering responsible AI that benefits society without undermining individual privacy.

AI originated in 1956 when John McCarthy created the term at the Dartmouth Summer Research Project.. According to Oxford Learner's Dictionary, "artificial intelligence is the study and development of computer systems that can mimic intelligent human behaviour'[1], which includes machine and deep learning.

According to 2(h) of Digital Personal Data Protection Act 2023, Data means a representation of informa-

[1] Oxford, *available at*: https://www.oxfordlearnersdictionaries.com/definition/english/artificial-intelligence (last visit on Sept 4 ,2024).

tion, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means".[2]

According to 2(n) of Digital Personal Data Protection Act 2023, "digital personal data means personal data in digital form".[3]

According to 2(t) of Digital Personal Data Protection 2023, personal data "means any data about an individual who is identifiable by or in relation to such data".[4]

According to 2 (u) of Digital Personal Data Protection 2023, "personal data breach" "means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data".[5]

2. Evolution of the Artificial Intelligence and Right to privacy

2.1 Artificial Intelligence (AI)

Countries around the globe are increasingly recognizing the economic and social potential of artificial intelligence (AI). For instance, China and the U.K. project that 26% and 10% of their respective GDPs in 2030 will stem from AI-related sectors. Over the past 18 to 24 months, several nations have made significant strides in defining AI policy and fostering AI ecosystems. The U.S. released its AI report in December 2016, followed by France's strategy in January 2017 and a comprehensive policy paper in March 2018 . Japan published its strategy in March 2017, China in July 2017, and the U.K. unveiled its industrial strategy in November 2017 .

Governments are prioritizing supply-side initiatives to build a robust AI ecosystem. Efforts include establishing "data trusts," enhancing digital infrastructure like 5G and full fiber networks, developing shared supercomputing resources, offering fiscal incentives, and promoting open-source software libraries , all of which are emphasized in national strategy documents.

In the realm of AI research, universities and institutions from the U.S., China, and Japan have led global research output between 2010 and 2016. U.S. institutions, including Carnegie Mellon, MIT, and Stanford, pioneered AI research by introducing specialized courses, setting up dedicated research centers, and forming industry partnerships. Recently, Chinese universities like Peking and Tsinghua have gained momentum through significant public funding and collaborations with private enterprises.

To prepare the workforce for the future of AI, nations are increasing investment in Science, Technology, Engineering, and Mathematics (STEM) education. Governments are enhancing university funding, introducing AI-focused courses, and implementing reskilling initiatives. For example, the U.K. aims to support over 1,000 PhD researchers by 2025, along with launching a Turing fellowship for AI experts , while China has initiated a five-year university program to train 500 teachers and 5,000 students in AI technologies.

[2] Digital Personal Data Protection Act 2023, India, *available at:* https://www.meity.gov.in/content/digital-personal-data-protection-act-2023 *(last visit on sept4, 2024).*

[3] Digital Personal Data Protection Act 2023, India, *available at:* https://www.meity.gov.in/content/digital-personal-data-protection-act-2023 *(last visit on sept4, 2024).*

[4] Digital Personal Data Protection Act 2023, India, *available at:* https://www.meity.gov.in/content/digital-personal-data-protection-act-2023 *(last visit on sept4, 2024).*

[5] Digital Personal Data Protection Act 2023, India, *available at:* https://www.meity.gov.in/content/digital-personal-data-protection-act-2023 *(last visit on sept4, 2024).*

Governance models to facilitate these efforts vary by country. Some have established dedicated bodies such as the UAE's Ministry of AI and the U.K.'s Office for AI and AI Council. Other countries, like China and Japan, have integrated AI initiatives within existing government ministries. Local governments are also increasingly investing in AI projects, recognizing their transformative potential.

Public funding for AI has surged, with governments like China, the U.S., France, and Japan significantly boosting R&D spending, establishing AI-focused funds for startups, and making large-scale investments in infrastructure and public procurement. Many nations are leveraging public-private-academic partnerships to drive AI development, including creating tech parks, connecting corporations with startups, and forming national teams with leading private players to advance both fundamental and applied research.

The rapid pace of AI development has far-reaching economic and societal implications . According to a study by EY and NASSCOM, by 2022, nearly 46% of the workforce will be employed in jobs that either do not exist today or have undergone significant skillset changes. Countries that delay in establishing AI strategies may struggle to catch up to the current momentum in this rapidly evolving environment. Consequently, it is crucial for nations like India to craft a comprehensive policy framework to build a thriving AI ecosystem.

2.2 Right to Privacy

The right to privacy has been a fundamental aspect of legal frameworks long before modern data protection regulations. Its roots trace back to constitutional provisions and key international agreements.

In 1789 The US Bill of Rights established the right to security in one's "person, houses, papers, and effects against unreasonable searches.

In 1890 Samuel Warren and Louis Brandeis introduced the concept of privacy as "the right to be let alone," with concerns over technology's impact on privacy.

In 1948The United Nations Declaration of Human Rights (Article 12) prohibited arbitrary interference with privacy.

In 1950The European Convention on Human Rights (ECHR) enshrined the right to private and family life, with certain restrictions for democratic society.

In 1974 In the US, the Family Educational Rights and Privacy Act (FERPA) and the Privacy Act established key protections for educational records and personal data.

1980: The OECD Guidelines on Privacy and Transborder Data Flows laid out principles like consent , access, and accountability for data privacy.

1981: Convention 108 became the first legally binding international agreement on data protection, regulating cross-border data flows.

1995: The EU Data Protection Directive introduced key privacy principles like transparency, later forming the basis for the GDPR.

1996-1999: US laws like HIPAA, COPPA, and the GLBA targeted privacy in healthcare, children's online safety, and financial information, respectively.

2002: The e-Privacy Directive addressed privacy in electronic communications, notably introducing cookie regulations.

2005: The APEC Privacy Framework provided guidance for businesses and governments across Asia-Pacific on privacy protection.

2012: The European Charter of Fundamental Rights further solidified privacy protections, distinguishing between general privacy and data protection rights.

2013-2020: The Schrems cases in the EU invalidated data transfer agreements like Safe Harbor and Privacy Shield, emphasizing the need for strict data protection in international transfers.
2014: The Malabo Convention aimed to harmonize cybersecurity and privacy laws across African Union members.
2016-2018: The GDPR came into force, setting a global benchmark for comprehensive data protection laws.
2020: The California Consumer Privacy Act (CCPA) marked a major step in US privacy law, giving consumers control over their personal data.
2021: China's Personal Information Protection Law (PIPL)introduced comprehensive privacy regulations , aligning with international standards.

The evolution of privacy rights continues, with legislation like the proposed American Data Privacy and Protection Act (ADDPA) potentially reshaping the US privacy landscape.

Nariman J. emphasized that the constitutional basis for privacy lies in the concept of human dignity, which includes an individual's right to fully realize their potential . This growth, however, can only occur when a person has control over key personal decisions and the sharing of their data, which could otherwise be compromised by unauthorized use.[6]

Article 21 of the Constitution has been interpreted by the courts to extend protection to individuals' personal information. However, the right to privacy is not absolute ; it can be subject to reasonable restrictions in order to safeguard national sovereignty, integrity, security, foreign relations, public order, decency, or morality. he landmark case of **"Justice K. Puttaswamy (Retd.) vs Union of India"**[7] marked a significant victory for the right to privacy. In this case, the constitutional validity of India's biometric identity scheme, Aadhaar, was challenged. It became a pivotal moment in Indian legal history, as the Supreme Court ruled that the right to privacy is a fundamental right. All nine judges on the bench unanimously recognized privacy as an essential aspect of the right to life and personal liberty under Article 21, and as a core part of the rights guaranteed under Part III of the Indian Constitution[8].

The safeguards surrounding personal information in India have notable gaps . Under Section 43A of the Information Technology Act, companies managing personally identifiable information must implement security measures, and failure to do so can lead to financial liabilities. The increasing data security concerns are heightened by the extensive use of data in various e-governance initiatives.

A promising step was taken by the Justice Sri Krishna Committee with the introduction of a new personal data protection law. This legislation emphasizes obtaining explicit consent from individuals before their data is processed or shared, whether within India or internationally. It also grants individuals the right to request the deletion of their data and exercise the "right to be forgotten." Non-compliance with the law may result in fines ranging from "Rs. 15 crores to 4% of a company's annual turnover [9].

3. Threat to Implement the AI in India

The earlier analysis of key sectors—Healthcare, Agriculture, Education, Smart Cities and Infrastructure, and Smart Mobility and Transport—underscores the significant potential of AI technologies in

[6] D. Majumdar and H.K. Chattopadhyay, "Emergence of AI and its implication towards data privacy: From Indian legal perspective," IJLMH, Volume 3 | Issue 4 (2020).

[7] AIR 2018 SC (SUPP) 1841

[8] Writ Petition (Supreme Court) (Civil) No.494 of 2012.

[9] "Artificial Intelligence and Laws In India," Legal Services India, (April 4, 2024) Available at:https://legalserviceindia.com/legal/article-8171-artificial-intelligence-and-laws-in-india.html (Last visit on 4th oct. 2024)

transforming these areas and, by extension, the Indian economy. However, it also identifies numerous challenges that India must overcome to fully harness the potential of such a disruptive technology.

When we examine these barriers from the lens of a single sector, they may seem specific and limited. For instance, in the Healthcare sector, widespread adoption of AI would require overcoming several hurdles, such as:

1. A lack of coordinated efforts among various stakeholders: Although India has introduced an electronic health record (EHR) policy, data sharing across different hospital networks remains limited, as each has its own interpretation of what "digitizing records" entails.
2. Insufficient availability of relevant data and the lack of comprehensive open clinical datasets.
3. Concerns over data privacy and security, including the absence of formal regulations on data anonymization.

However, when these challenges are considered across various sectors, common themes begin to emerge:

1. Lack of well-developed data ecosystems
2. Insufficient AI research intensity, both in fundamental technologies and their market applications
3. Shortage of AI expertise, skilled professionals, and training opportunities
4. High resource costs and limited awareness of AI’s business applications
5. Ambiguity around privacy, security, and ethical standards
6. An intellectual property regime that is not sufficiently attractive to encourage AI research and adoption

Although this list of challenges is not exhaustive, addressing them through collaborative efforts among stakeholders, with the government taking a leading role, could establish essential foundational elements for India’s progress in AI.

4. Suggestion

India's approach to harnessing the potential of artificial intelligence (AI) must be carefully balanced to address both its domestic challenges and its ambition to take a leadership role globally . This balance requires large-scale, transformational efforts driven primarily by the government, with strong support from the private sector. India’s AI strategy should focus on addressing pressing local needs while also contributing to the global AI landscape.

The following recommendations outline how India can address its key challenges and capitalize on AI's opportunities. The analysis of key sectors indicates that efforts should concentrate on four major themes: advancing research, democratizing data, accelerating AI adoption, and reskilling the workforce. At the same time, privacy, security, ethics, and intellectual property (IP) must remain central considerations across all initiatives. By addressing these challenges with a collaborative approach involving all stakeholders—and with the government playing a crucial role—India can lay the groundwork for its AI vision of "#AIforAll."

India's current capabilities in AI research are limited, both in terms of volume (ranking 5th globally) and , more critically, in the quality and impact of the research produced. The AI research community is concentrated in a few academic institutions and relies heavily on individual talent rather than institutional excellence. Private sector contributions to AI research have also been minimal. Although some encouraging steps have been taken—such as the Government of Karnataka's collaboration with NASSCOM to establish an AI Centre of Excellence—much more needs to be done. The first set of recommendations focuses on significantly boosting both core and applied AI research. Two frameworks are also proposed to tackle some of AI's biggest research challenges through a collaborative, market-oriented approach.

The advent of AI and other cutting-edge technologies will disrupt the future of work, creating demand for new skills while making some jobs obsolete due to automation. This workforce transformation will require addressing both demand and supply challenges—demand for skills in jobs that don't yet exist and the oversupply of STEM graduates, many of whom may struggle to find meaningful employment. While India's IT sector and favorable demographic profile might appear to provide an advantage, the sheer scale of the population means that without the right structures in place, this potential could become a liability. The next set of recommendations focuses on reskilling the existing workforce and preparing students with practical skills for the evolving technological landscape Early adoption of AI—whether by the research community, startups, or corporations deploying AI solutions—will be critical to achieving leadership in AI. However, AI adoption in India has been limited ; less than a quarter of Indian companies currently use AI in their business processes, and the AI startup ecosystem is still in its infancy. Key barriers to widespread AI adoption include limited access to structured data, the high cost and limited availability of computing infrastructure, and a lack of collaboration and awareness. To address these challenges, it is recommended that India develop large, annotated datasets to democratize data and create multi-stakeholder marketplaces across the AI value chain, from raw data to AI models.

A fundamental element of India's #AIforAll vision is responsible AI, which ensures that concerns related to privacy, security, and intellectual property are addressed while balancing ethical considerations with the need for innovation. The final set of recommendations outlines strategies for addressing the complex challenges associated with implementing AI in a responsible and sustainable manner.

These recommendations are intended to initiate a comprehensive dialogue on India's future AI roadmap. They are designed to be descriptive rather than prescriptive, providing a framework for developing a National Strategy for AI. Specific funding targets and mechanisms have not been included, as these will require further discussions with stakeholders across sectors.

5. Conclusion

The rise of artificial intelligence (AI) holds tremendous potential for advancing society , but it also presents significant challenges in safeguarding privacy rights . As India undergoes rapid digitization and increasingly adopts AI across various sectors, it is imperative for the government to take proactive steps to address privacy concerns. Striking a balance between encouraging innovation and protecting fundamental rights, like privacy, will be essential. The Digital Personal Data Protection (DPDP) Act of 2023 represents a key step forward in establishing a comprehensive data protection framework in India . However, questions persist about potential exemptions for government agencies and whether the Act adequately addresses AI-specific issues. To foster responsible AI development that delivers socio economic benefits while upholding individual privacy , it is crucial to have robust governance frameworks, ethical standards, and regulatory sandboxes. Courts have recognized the importance of balancing privacy rights with legitimate governmental objectives, such as national security, in landmark decisions. Applying this principle to AI requires a sophisticated, context-specific approach that encourages innovation while ensuring the protection of individual privacy. Since AI systems depend heavily on vast amounts of personal data for training, strong data security and privacy-preserving practices must be incorporated throughout the AI lifecycle.

India should also keep pace with global developments and best practices for managing AI's impact on privacy. As data crosses borders and privacy regulations extend beyond national boundaries, there is a need for harmonized and mutually recognized regulatory frameworks. India must prioritize the development of responsible AI that aligns with democratic values and human rights, establishing itself as a global leader in technology. Ensuring privacy in an AI-driven world will require a collaborative approach involving multiple stakeholders, including government, industry, civil society, and individuals. Continuous public engagement, enhancing knowledge and skills, and raising awareness of privacy rights are essential to navigating this technological transformation in a just and ethical manner. India's future as a true knowledge leader will depend on its ability to find the right balance between privacy protection and AI innovation.

6. References

1. Right to Privacy vis-à-vis Artificial Intelligence: Indian Scenario.
2. https://oecd.ai/en/wonk/india#:~:text=Driven%20AI%20entrepreneurs%20power%20their%20skilled%20AI%20workforce,itself%20as%20an%20AI%20research%20and%20innovation%20powerhouse.
3. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
4. Kruthika R. The Right to Privacy in Indian Constitutional History. CAD. India Blog.
5. Hutton E. J. (1976). The Right of Privacy in the United States, Great Britain and India in Richard P. Claude (ed.). Comparative Human Rights. P. 151.