Page 748 - 755 **DOI:** *https://doij.org/10.10000/IJLSI.112667*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 3

2025

The Study of Data Protection Laws in the Era of Artificial Intelligence

DR SIBANI SARMAH[1]

ABSTRACT

In recent years, artificial intelligence (AI) has experienced significant advancements. Currently, AI tools are being utilized more frequently by organizations in both the private and public sectors worldwide. The potential of AI today and in the foreseeable future offers considerable advantages for individuals, institutions, and society as a whole. Nevertheless, these technological advancements also present critical challenges, particularly regarding the relationship between AI and data protection regulations. Consequently, we face both a chance and a responsibility to assess the adequacy of existing data protection laws in the context of contemporary technological developments. The relationship between artificial intelligence (AI) and data protection legislation is becoming more complex, leading to various legal and ethical dilemmas. Although current data protection regulations, such as the Digital Personal Data Protection Act (DPDP) in India, are designed to protect personal information, they may not adequately tackle the distinct challenges that AI presents. This paper explores the existing data protection laws in India as well as examine the legal framework ,statues and case laws related to AI .The paper also evaluates the strength and weakness of the existing legal framework and provides a recommendation to address the challenges of AI and data protection.

Keywords: *Artificial intelligence, Data protection, Laws, Statute*

I. INTRODUCTION

Artificial intelligence (AI) is a term used to describe the process of machines and computers performing tasks that typically require human intelligence, like learning. It may sometimes feel like AI is a recent development in technology. But it has been observed that foundation for artificial intelligence was established in the early 20th century. While significant advancements did not occur until the 1950s, these developments were made possible by the contributions of early specialists across various disciplines.

Warren McCulloch and Walter Pitts created a model of artificial neurons, which is regarded as the pioneering form of artificial intelligence. Alan Turing's research on 'Computing Machinery and Intelligence' established the Turing Test, a standard for evaluating machine intelligence.

[1] Author is an Assistant Professor at Mahatma Gandhi University Meghalaya, India.

 [ISSN 2581-9453]

In 1950, British mathematician Alan Turing wrote an article called "Computing machinery and intelligence" in the magazine Mind, where he questioned if machines can think. He suggested an experiment known as the Turing Test to see if a machine could behave intelligently like a human. In 1956, John McCarthy introduced the term "artificial intelligence" and helped create the first AI programming language, LISP, in the 1960s. Early AI systems focused on rules, leading to more advanced systems in the 1970s and 1980s with increased funding. Today, AI is thriving due to improvements in algorithms, hardware, and machine learning.

In recent years, this technology has experienced significant growth, largely driven by advancements in deep learning. Currently, AI tools are being utilized more frequently by organizations in both the private and public sectors worldwide. The potential of AI today and in the foreseeable future offers considerable advantages for individuals, institutions, and society as a whole. Nevertheless, these technological advancements also present critical challenges, particularly regarding the relationship between AI and data protection regulations.

Artificial Intelligence is also utilized in combating fraud and has created an opportunity for businesses to implement due diligence, prudence, and care.

The utilization of personal data by AI systems can have a range of effects on individual privacy, including:[2]

Intrusion: AI systems might gather and process personal data without the awareness or consent of the individuals involved, or in manners that exceed their reasonable expectations. For instance, AI systems could employ facial recognition technology.

Profiling: AI systems may leverage personal data to construct profiles of individuals or groups, enabling them to make predictions, recommendations, or decisions regarding those individuals. For example, AI systems might utilize personal data to evaluate the creditworthiness, employability, health status, or personality traits of individuals, or to direct personalized advertisements, offers, or services towards them.

Discrimination: AI systems may utilize personal data to differentiate or unfairly treat individuals or groups based on their characteristics, such as age, gender, race, ethnicity, religion, or disability..

II. DATA PROTECTION AND IT'S EFFECTS ON AI

Data protection encompasses a collection of legal regulations and principles designed to safeguard the rights and freedoms of individuals concerning their personal data.

[2] https://seifti.io/ai-and-data-protection-law/

Legislation on data protection, including the General Data Protection Regulation (GDPR) in the European Union and the Data Protection Act 2018 in the United Kingdom, governs the collection, processing, and dissemination of personal data by entities such as public authorities, private enterprises, or non-profit organizations.

The influence of data on AI systems can be observed in numerous aspects, such as [3]

Data minimization: Data protection regulations stipulate that personal data gathered and processed by AI systems must be adequate, pertinent, and confined to what is essential for the intended purposes of processing.

Lawfulness, fairness, and transparency: This indicates that AI systems must possess a legitimate legal foundation, such as consent, contractual obligation, or public interest, for the collection and utilization of personal data, ensuring that they do not infringe upon the rights and interests of individuals. Furthermore, AI systems are required to furnish clear and accessible information to individuals regarding the collection, usage, and sharing of their personal data, as well as their rights and options concerning their personal data.

Accuracy: This implies that AI systems must guarantee that the personal data they utilize is accurate, complete, and relevant, and they should rectify or eliminate any incorrect or outdated personal data.

Security: This signifies that AI systems must adopt technical and organizational measures, including encryption, authentication, or access control, to safeguard the personal data they handle from unauthorized access, disclosure, modification, or deletion.

III. THE DATA PROTECTION FRAMEWORK IN INDIA

Until 2023, India lacked a specific law or framework for data protection. The Information Technology Act of 2000 (IT Act) and its associated rules were the foundation of the data protection framework. This included the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules from 2011 (Privacy Rules).

In 2017, a constitutional bench of nine judges from the Supreme Court of India ruled in Justice K. S. Puttaswamy (Retd.) v. Union of India [4]that privacy is a fundamental right, protected under Article 21 [Right to Life & Liberty] of the Indian Constitution. This decision initiated the development of a comprehensive data protection framework for India. After releasing various

[3] Ibid
[4] Writ Petition No. 494/ 2012

draft versions of data protection legislation and taking into account feedback from different stakeholders, the Ministry of Electronics and Information Technology (MeitY), Government of India, published the draft of the Digital Personal Data Protection Bill in 2022 (DPDP Bill).

On August 11, 2023, the Indian Government announced the Digital Personal Data Protection Act, 2023 (DPDP Act), which will establish the framework for personal data protection and regulation in India. The DPDP Act brings in various requirements regarding the collection, processing, storage, and transfer of digital personal data.

The DPDP Act is based on these principles:[5]

1. Organizations must use personal data in a lawful, fair, and transparent way for the individuals involved;
2. The use of personal data should be restricted to the purpose for which it was originally collected;
3. Only the personal data necessary for achieving a specific goal should be gathered;
4. Reasonable efforts must be made to ensure that individuals' personal data is accurate and up to date;
5. Data storage should be limited to the time necessary for the stated purpose of collection;
6. Reasonable measures must be taken to prevent unauthorized collection or processing of personal data, aiming to avoid data breaches;
7. The individual who determines the purpose and methods of processing personal data, known as the Data Fiduciary, is responsible for that processing.

The DPDP Act is not applicable to (i) personal data used by an individual for personal or household purposes or (ii) personal data intentionally made publicly available by either the Data Principal to whom the personal data pertains or any other individual or entity required by law to disclose personal data to the public.

Key Challenges and Loopholes:[6]

While the DPDP Act establishes a fundamental legal framework for the protection of digital personal data, numerous uncertainties persist regarding the emergence of AI technologies. Below are several critical areas of concern where both subjects intersect, revealing potential risks and vulnerabilities:

[5] Data protection in India,2025, retrieved from https://www.dlapiperdataprotection.com/?t=law&c=IN

[6] https://www.barandbench.com/view-point/the-confluence-of-ai-and-data-privacy-aligning-data-privacy-regime-in-india-for-the-age-of-ai

1. **Section 7 and Public Interest Loopholes:** Section 7 permits data processing without consent for the sake of "public interest," yet the ambiguous nature of this term creates opportunities for misuse. For example, the Delhi Police employed facial recognition technology during the anti-CAA protests, justifying it on the grounds of public safety. Such surveillance poses a risk of violating Article 21 (Right to Life and Personal Liberty) by facilitating non-consensual tracking and profiling without adequate legal protections or accountability.

2. **Automated Decision-Making and Accountability Gaps**: The Act does not provide sufficient clarity regarding AI-driven decision-making and the associated accountability. For instance, failures in Aadhaar-linked biometric systems within welfare programs such as PDS and MGNREGA have resulted in the denial of services, disproportionately affecting marginalized communities and raising issues under Article 14 (Right to Equality), all while lacking a clear mechanism for addressing algorithmic discrimination.

3. **Cross-Border Data Transfer Restrictions:** The limitations imposed by Section 17 on cross-border data transfers, along with MeitY's advocacy for data localization, obstruct global AI collaboration and increase compliance expenses. For example, proposed regulations necessitate that companies such as Amazon, Google, and Facebook retain Indian user data within the country, which restricts access to international AI resources and disproportionately affects startups and developers.

4. **Consent Mechanisms and Transparency Challenges:** The complexities inherent in AI systems often render it difficult for users to give informed consent. Government platforms such as UMANG and MyGov utilize AI chatbots; however, they lack transparency concerning data usage, storage, and sharing, which undermines the fundamental principle of informed consent as outlined in the DPDP Act.

Limitations of IT Act,2000:

The Information Technology Act of 2000 marked India's initial significant digital legislation, aimed at fostering e-commerce, addressing cybercrime, and providing legal recognition to electronic communications.

Although it functioned effectively during the early internet period, it was not crafted to tackle the intricacies of artificial intelligence and contemporary digital environments. Numerous Sections of the Act now seem outdated. For instance, Section 43A, which requires compensation for the failure to safeguard sensitive personal data, does not take into account the specific risks associated with AI. Section 66 imposes penalties for individual cybercrimes

but fails to address wider systemic issues such as AI-driven misinformation and algorithmic manipulation.

The previously existing Section 66A, which was invalidated in the case of Shreya Singhal v. Union of India due to its vagueness and unconstitutionality, has created a regulatory void concerning harmful AI-generated content, deepfakes, and synthetic media. Furthermore, Section 69, which allows for surveillance under the guise of national security, does not include specific protections against invasive AI technologies like facial recognition and predictive analytics, thus raising significant privacy issues under Article 21 of the Constitution.

Moreover, Section 79 offers safe harbour to intermediaries but neglects to account for the proactive role that AI plays in content curation and amplification, thereby diminishing platform accountability.

Given these existing shortcomings, there is a distinct necessity for a thorough and forward-thinking regulatory framework.

IV. IMPORTANT CASE LAWS RELATING TO DATA PROTECTION

Here are some notable case laws related to data protection:

Justice K.S. Puttaswamy and Anr vs. Union of India (2018): This landmark case recognized the right to privacy as a fundamental right under the Indian Constitution. The Supreme Court discussed the validity of the Aadhaar Act and its implications on individual privacy.

Rochem Separation System Pvt. Ltd. V. Nirtech Pvt. Ltd. And Ors. (2022): The Bombay High Court granted an ex parte injunction against an ex-employee who misused confidential company data, including client information and pricing details, after joining a competitor.

Aaradhya Bachchan & Anr vs. Bollywood Times and Ors. (2023): The Delhi High Court issued directives to protect Aaradhya Bachchan's personal data and prevent non-consensual sharing of intimate images online. The court emphasized intermediaries' responsibility to remove such content upon receiving court orders.

These cases highlight the growing importance of data protection laws in India, particularly with the increasing use of artificial intelligence and digital technologies.

V. RECOMMENDATIONS FOR DATA PROTECTION LAWS IN INDIA

1. Develop a robust and comprehensive data protection law that addresses the unique challenges posed by emerging technologies like AI, and big data analytics.

2. Provide clear definitions of key terms, such as personal data, sensitive personal data, and data processing, to avoid ambiguity and ensure consistency in interpretation.
3. 3.Establish effective consent mechanisms that allow individuals to make informed decisions about their data, including the right to withdraw consent and opt-out of data collection.
4. Encourage data minimization practices to reduce the risk of data breaches and unauthorized use.
5. 5.Ensure transparency in data collection, processing, and usage, and establish clear accountability structures to hold organizations responsible for data protection.
6. 6.Establish robust enforcement mechanisms and impose significant penalties for non-compliance to deter data protection violations.
7. 7.Develop guidelines for cross-border data transfers to ensure that data is protected when transferred outside India.
8. Launch public awareness campaigns to educate individuals about their rights and responsibilities under the data protection law.

VI. CONCLUSIONS

In conclusion, effective data protection laws are crucial in today's digital age to safeguard individuals' personal information and promote trust in the digital economy. By enacting and enforcing strong data protection laws, governments can protect citizens' rights, foster innovation, and support economic growth in the digital era.

By implementing these recommendations and conclusions, India can develop a robust data protection law that protects individual rights, promotes trust in the digital economy, and supports the country's economic growth and development

******

 [ISSN 2581-9453]

VII. REFERENCE

- Zahrasadat Naghibzakerin, Mitra Shahabsafa, Mohammadreza Mollahoseini Ardakani, Kamal Mirzaie, & Seyed Alireza Azimidokht Shooroki. (2025). Analysis of Legal Challenges and Data Protection Strategies in the Era of Artificial Intelligence in the International Legal System. 4(2), 21–38. https://doi.org/10.61838/kman.isslp.
- Jolly, R., Singh, P., & Kumar, A. (2025, May 9). The Confluence of AI and Data Privacy: Aligning Data Privacy Regime in India for the Age of AI. Bar and Bench – Indian Legal News. https://www.barandbench.com/view-point/the-confluence-of-ai-and-data-privacy-aligning-data-privacy-regime-in-india-for-the-age-of-ai
- DLA Piper. (2024). Data Protection Laws in India – Data Protection Laws of the World. Dlapiperdataprotection.com. https://www.dlapiperdataprotection.com/?t=law&c=IN
- Fernández, J. A. (2024, February 19). AI and Data Protection Law – Seifti. Seifti. https://seifti.io/ai-and-data-protection-law/

*****