An analysis of specific legislations and regulations governing the developing AI in India.

Dr. Asmita Patil Assistant professor Shahaji Law College, Kolhapur

---

Abstract:

Artificial intelligence is a complex and multifaceted issue. AI systems rely on large amount of personal data, which erode individual's right to privacy. Any sector powered by AI leads to loss of autonomy, which also leads to stigma and discriminations against marginal groups. Hence in India we see various regulations controlling the ill-effects of AI. General data protection regulation, Data protection impact assessments, Human centric AI design are some such regulations. Digital Personal Data Protection Act (DPDPA) of 2023, is one such legislations which gives an umbrella coverage to curb the infringing the right to privacy. The present research paper gives a detail analysis of how the act will withstand the ill-effects of violation of right to privacy.

Key words: AI, right, privacy, data.

Introduction:

"The measure of intelligence is the ability to change" Albert einstein. As said in the quote, the power of artificial intelligence is so incredible, it will change the society in some very deep ways. Artificial intelligence is a field of study that uses machines to mimic human intelligence. AI can learn, reason and act in the ways as humans do. AI learns and improves by analyzing large amount of data. Very common examples used today are voice assisted smart phones, financial trading, language translation, chess playing computers as well as self-driving cars. Artificial intelligence is a complex and multifaceted issue. AI systems rely on large amount of personal data, which erode individual's right to privacy. Any sector powered by AI leads to loss of autonomy, which also leads to stigma and discriminations against marginal groups. Hence in India we see various regulations controlling the ill-effects of AI. General data protection regulation, Data protection impact assessments, Human centric AI design are some such regulations. Digital Personal Data Protection Act (DPDPA) of 2023, is one such legislations which gives an umbrella coverage to curb the infringing the right to privacy. The present research paper gives a detail analysis of how the act will withstand the ill-effects of violation of right to privacy.

Research questions:

- What is the impact of AI on right to privacy.
- What are the measures to strengthen and protect the right to privacy.

Objectives of study:

- To research the impact of AI on right to privacy
- To determine the measures to strengthen and protect right to privacy

Significance of study:

In the present research, there is an attempt made to study the impact of AI on right to privacy. As now-a-days with the development of AI in almost all the fields there is a large problem of personal data security. In India we see different sectors which were affected by the encroachment of AI and data sealing. To curb such insecure practices, the government has brought up many legislations as well as regulations which are controlling AI and keeping it in clutches.

Research methodology:

The research methodology which has been used in present research is doctrinal. Doctrinal research includes analyzing case-laws, organizing, ordering and systematizing legal ideas as well as studying the legal institution. As a result, the procedure utilized here requires study of theoretical content, the practical approach towards the problem supporting it with legislative issues. The primary sources used in the research paper are various cases and the legislative enactments present in India. The secondary sources include scholarly books, research reports, journals, dissertations, textbooks and various websites.

Conceptual analysis:

Artificial intelligence can be said to be the theory and development of computer systems that are capable of performing tasks that require human intelligence like recognizing speech, making decisions and identifying patters. Some of the most common examples used today are Chat GPT, Google Translate, Netflix, Tesla etc. Artificial intelligence has acquired nearly all fields, as it does not require human intervention and it saves money as well as time. As it has many potential benefits, like great accuracy, decreased operational costs, improved decision making, it also has many potential dangers like, loss of employment due to increased automation, cyber security concerns as well as infringement of right to privacy.

Concerns of AI systems:

1. Data collection and surveillance: AI systems often rely on vast amounts of personal data, which can erode individuals right to privacy.
2. Predictive analytics and profiling: AI powered predictive analytics can create detailed profiles of individuals, potentially infringing on their right to privacy and autonomy.
3. Bias and discrimination: AI systems can perpetuate existing biases and discriminate against certain groups, further exacerbating privacy norms.
4. Lack of transparency and accountability: AI decision making processes can be opaque, making it difficult to hold organizations accountable for privacy violations.

Impact on individuals:

1. Loss of autonomy: AI driven surveillance and profiling can limit individuals' freedom to make choices and live their lives without unnecessary scrutiny.
2. Stigma and discrimination: AI powered profiling can perpetuate stigma and discrimination against marginalized groups.
3. Erosion of trust: repeated privacy violations can erode trust in institutions and organizations, undermining social cohesion.

Regulatory frameworks and solutions:

1. General data protection regulation (GDPR): the GDPR provides a framework for protection of individuals personal data and privacy in the EU.
2. Data protection impact assessments (DPIAs): DPIAs can help identify and mitigate privacy risks associated with AI systems.
3. Explainable AI (XAI) : XAI techniques can increase transparency and accountability in AI decision making process.
4. Human centric AI design: Designing AI systems with human values and privacy in mind can help mitigate potential risks.

Directions for regulating the increasing privacy risks of AI:

1. Developing AI Specific regulations: Government and organizations must create regulations tailored to the unique challenges posed by AI.
2. Investing in AI Ethics research: researching AI ethics and privacy can help develop more responsible and human centric AI systems.
3. Promoting transparency and accountability: Encouraging transparency and accountability in AI development and deployment is crucial for protecting individual's right to privacy.

What is right to privacy?

The right to privacy refers to an individual's entitlement to maintain the secrecy of their personal information, activities and physical space, which are not of legitimate public interest. This right ensures that people can live in society without unwanted disturbances or intrusion.

From constitutional rights to data protection:

Control over shared information, decision making and personal limits are made possible by privacy and widespread use of technology in the modern era poses serious privacy issues, which has led to international legislative initiatives to safeguard personal information. However effective lawmaking is challenged by rapid technical breakthroughs such as deep fakes powered by AI. this demands the constitutional acknowledgement of the right tp privacy in India under the right to life and international privacy rules that aim to safeguard people's freedom from exploitation and preservation of dignity.

Privacy --a right:

The UDHR adopted by the United Nations general assembly in 1948, enshrines Article 12 proclaiming that, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honor and reputation." The international covenant on Civil and political rights (ICCPR) adopted in 1966 provides through article 17 that, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation".

Right to privacy in India:

The evolution of right to privacy within India has emerged from the judiciary, marked by pivotal precedents who gradually solidify its recognition as a fundamental right under article 21. In Gobind V State of MP in 1975, the Supreme court introduced the compelling state interest test, emphasizing that privacy rights should yield to larger state interests only if convincingly justified.

PUCL V Union of India, in 1997, commonly referred to as telephone tapping case, in this case supreme court recognizes individuals' privacy interest in the context of their telephone communications, further reinforcing the acknowledgment of privacy rights within the ambit of constitution.

Further in 2017, Justice K.S. Puttaswamy V union of India, privacy attains its formal recognition as a fundamental right. SC unanimously declared privacy as an intrinsic part of life and personal liberty under article 21 which established a firm foundation for its protection.

Data protection in India:

In recent times there are several instances where date of millions of Indian users were breached.

1. One such incident in which an automated account on the messaging platform Telegram, allegedly sharing sensitive personal information, such as Aadhar and passport numbers of

individuals registered on the Cowin portal for Covid-19 vaccination. The Indian computer emergency team is actively investigating this matter.

2. A leaked database uploaded on GitHub claims to contain data from various Indian institutions including government and private entities, such as Employees Provident Fund organization, BSNL users' data and information from companies like Air India and Reliance.

3. 110 million customer's personal information from the mobile wallet and payment software Mobi Kwik is for sale on a dark web hacker site. This data set which contains over 8.2 terabytes of data, contains information about credit card details, Adhar card, KYC documents and cell numbers connected to Mobi Kwik wallets.

Indian legislation:

Information technology act 2000- instructions about storing and protecting data

The personal data protection bill proposed by BN Srikrishna committee in 2007, after being revised, it has reintroduced in 2023 as Digital Personal Data Protection Act 2023.

The primary legislation in India aimed at protecting data from AI is the Digital Personal Data Protection Act (DPDPA) of 2023, which governs the collection, processing and storage of personal data, impacting how AI systems can handle user information.

Key points about the DPDPA:

Comprehensive framework: the DPDPA establishes a broad set of rules for data protection, including provisions relating to consent, purpose limitation, data minimization and data breach notification, all relevant to AI applications.

No specific AI provisions: while the DPDPA is considered crucial for AI data protection, it does not explicitly address unique AI related challenges like automated decision making or algorithmic transparency.

Impact on AI companies: companies utilizing AI to process personal data must comply with the DPDPA's requirements, including obtaining user consent and implementing robust data security measures.

The DPDPA may also influence where sensitive data is stored, impacting cross-border data transfers by AI systems.

How can a data be protected: a data can be protected by some of the following regulations like, Data anonymization: to protect privacy, use anonymized datasets for training AI models. Synthetic data: generate synthetic data that mimics real data without containing personal data. Data minimization: collect and use only the data necessary for the specific AI application.

What does the DPDPA do:

- It establishes a framework for how personal data can be collected, processed, stored and transferred
- It gives individuals more control over their personal data, including right to access, correct and delete it.
- It allows for cross border data transfers to certain countries with similar data privacy laws
- It gives the government the power to regulate and restrict data transfer in certain circumstances.

Impact of DPDPA on data protection in India:

The digital data protection act significantly enhances data protection in India by establishing a comprehensive framework that empowers individuals with greater control over their personal information, holds organization accountable for data management and mandates stricter data

handling practices, particularly for sensitive data, thereby creating a more secure digital environment in India. individuals now have the right to access, rectify, erase, and restrict processing their personal data, requiring organizations to obtain verifiable consent before processing any information. Organizations must collect only the necessary personal data for the stated purpose and must erase data once the purpose is served, promoting responsible data collection practices. Organizations are required to report data breaches to the Data protection board within a specified timeframe and take necessary steps to mitigate the impact on affected individuals. Certain large scale data processor is classified as "Significant Data Fiduciaries" are subject to additional compliance requirements, including a data protecting officer.

Conclusion:

Thus, the digital data protection act ensures that the data stored is processed fairly and lawfully. The act compels the individuals to take charge of their personal data, enabling businesses to process it lawfully. It can be said that the DPDPA act represents a crucial step towards ensuring data protection and digital privacy in India. By empowering individuals with greater control over their personal information and holding organizations accountable for data management. Thus, the act tries to secure more secure digital environment.

References:

1. The digital data protection acts 2023 – the bare act
2. https://iapp.org, operational impacts of Indias DPDPA
3. https:// usercentric.com, Overview of DPDPA act
4. https://secureprivacyDPDPA explained.
5. https://sicencedirect .com
6. The Indian express.