

Bennett Journal of Legal Studies
Vol. 07(01), Feb 2026, pp. 145 – 158

ARTIFICIAL INTELLIGENCE CONSUMER PROTECTION AND REGULATORY CHALLENGES OF DATA PRIVACY

Dr. Priya Vijay

Assistant Professor of Law, Faculty of Law, University of Allahabad, Prayagraj, Uttar Pradesh, India

Disha Kalra

Advocate, High Court of Delhi

ABSTRACT

The paper is an attempt to highlight the grave concern arising from extensive use of Artificial Intelligence (AI) in all magnitudes of our lives and the impact it creates. The process of collection and processing of data is significantly unregulated and suffers from lack of sufficient safeguards. The paper provides a thorough reference to other potential jurisdictions who have better system of governance of data so as to protect consumer rights. Consumer data compromise and breach raise serious objection on the way the AI is allowed to be used and interfere with our freedoms. The paper addresses the concerns of breach of the data and also seeks to point out that such concerns can be resolved in the light of International best practices. Indian legal system needs to evolve in the light of global changes. Though complete adoption of laws is not conducive in Indian scenario but its assimilation as per Indian needs is required. The means must grow to ensure protection of privacy and accountability in data governance. The Digital Personal Data Protection Act, 2023 cannot be said to be satisfactory enough to guarantee the safeguard against consumer data breaches.

Keywords - AI – Privacy – Consumer - Breach of Data - The Digital Personal Data Protection Act, 2023

1. INTRODUCTION

Rampant use of AI has drastically changed the way, data is collected from the consumers, is, gathered and used in various fields like banking, finance, and healthcare. These technologies allow for greater efficiency and personalization, but, on the other side of the coin, raises serious

concerns for privacy, security and greater autonomy. In today's digital landscape, consumers' interaction with AI are seamless, without having complete knowledge and information as to how the data that is collected is used. These interactions may be in the form of personalised data collection, automated credit evaluation among others.

While the European Union General Data Protection Regulation, has set a global benchmark for the protection of privacy and accountability in data governance, many countries, to which India is not an exception, are still in the process of developing their regulatory framework. The introduction of The Digital Personal Data Protection Act, 2023 marks an important milestone in that process. However, debate continues as to how effectively the law addresses the challenges associated with AI, whether its enforcement mechanisms are good enough, or, how well it can protect its consumers in rapidly transforming digital environment.

There is a need to study the three-way interrelationship between AI, consumer data, and privacy rights with special focus on Indian scenario, and, also to explore how far existing legal and ethical frameworks would safeguard the interests of the consumers from the newly emanating risks associated with the AI- driven technologies. This study intends to, highlight the prevailing gaps in the regulatory framework and suggest some technological and policy measures that can help in promoting a more transparent, accountable, and rights-oriented AI landscape.

2. ORIGIN OF AI

AI is a term coined by McCarthy, is a branch of computer science intended to develop machines and system that perform certain tasks and activities, imitating human intelligence. Machines led by AI technologies has enabled data learning and implementing tasks requiring pictorial choice, audio identification and judgement which would otherwise would be performed by human agency.¹ The Ministry of Electronics and Information, defines AI, as, "a cluster of technologies that enable machines to work with a high level of intelligence, and, copying human capabilities of comprehending things and act."²

AI is often, referred as a "double-edged sword in terms of its impact on privacy".³ In comparison to conventional means the use of AI led technology safeguards against cyber offences and saves the personal data from being exposed to various forms of vulnerability. But,

¹ Maan, S., & Sharma, A. "PROTECTING CONSUMER RIGHTS IN THE AGE OF AI: LEGAL IMPLICATIONS AND CHALLENGES IN CONSUMER PROTECTION (2024) Atlantis Press 511

² The Ministry of Electronics and Information

³ Dr. Kalada D.S. Nonju and Agent Benjamin Ihua-Maduenyi
Faculty of Law, University of Port Harcourt, Rivers State, Nigeria, The Impact of AI on Privacy Laws (2024)
IJRISS 2150-2174

on the other hand, it also raises serious concerns related to privacy, because of its mass surveillance and data analysis capabilities. Many government and private entities have started using the ‘face-recognition technology’⁴ which is enabled by AI for the purpose of surveillance. While many of these face-recognition systems, are, purportedly being used for the purpose of surveillance and for security reasons, they often do so without any form of significant oversight, thus eventually raising serious concerns for mass surveillance and breach of privacy rights.⁵

AI has been increasingly used in various sectors, like, healthcare, finance, banking etc. AI systems are powered by algorithms and large sets of data and can be trained to perform particular tasks by recognising a pattern in the tasks. Virtual assistants, like SIRI and Amazon Alexa are common examples of the application of AI.⁶ With the introduction of AI, various changes have been introduced in the consumer markets, like the way the goods are produced, marketed and consumed. AI techniques like personalised suggestion, dynamic pricing and automated consumer service have increased the efficiency of the consumer relationship. However, these developments in the AI, also raises serious concerns on privacy of the consumer, transparency, and the liability of the consumer.⁷

Overall, AI is a fast-growing field with the potential to revolutionise the industries by improving the efficiency, accuracy and automation for various tasks that can help the consumers. However, with the rampant advance of AI, and it’s growing involvement in the lives of the people, raises serious apprehensions. Hence, there is an urgent need to keep pace with the ever-evolving technology of AI. It has been suggested that there is an urgent need to implement new measures which suggest that there is an urgent need to implement new countermeasures.⁸ One of the subsets of AI is, Machine- language, i.e., “the ability to learn without being explicitly programmed.”⁹ The term was coined by Arthur Samuel in 1959. Machine language makes the use of algorithms to analyse the data and thereby making a prediction.¹⁰

3. AI & CONSUMER PROTECTION

⁴ Ibid note 3.

⁵ Ibid note 3.

⁶ Supra note 1.

⁷ Ruchi Agarwal, The Role of AI in Consumer Protection Act in Current Scenario (2025) LAWCTOPUS

⁸ Supra note 1.

⁹ National strategy for AI #AI FOR ALL June 2018 Niti aayog

¹⁰ Ibid note 9

The consumer policy deals in safeguarding the rights and interest of the consumers in the marketplace. In India, The Consumer protection Act, 2019 provides for a legal framework for the protection of the consumer rights. The Consumer Protection Act, 2019 provides for various rights of the consumers, their protection, and also establishes various authorities for the redressal of consumer disputes. The statute deals with a wide array of issues, relating to goods, services, product liability. It tends to maintain the trust of the consumers in commercial transactions.¹¹

With the recent technological advancements, and with the growing use of AI, in handling consumers information the serious concerns of privacy and fraudulent actions are rising rapidly. The rapid growth of technology poses significant challenges to protect personal data and maintain information security.¹² But, on the other side of the coin, AI techniques like personalized suggestion, dynamic pricing etc. enhance efficiency and consumer bonds.

AI interacts with the consumers on a daily basis through various means, which are designed to promote ease, convenience and targeted personalisation. Various virtual assistants like Amazon's Alexa, Samsung's Bixby and Apple's Siri provide a platform, for the AI, to interact with the consumers, like by answering their questions, interacting with them, providing them with recommendations etc. These personalised user experiences are tailored by user's preferences and behaviours. The AI-driven chatbots, which are constantly evolving according to the needs of the people, provide for immediate support to consumers, for the resolution of any form of issue.¹³

The Consumer Protection Act, 2019, i.e., CPA, 2019, provides for the protection of consumer rights. The Act talks about various provisions, like, unfair contacts, trade practices etc. and also provide for regulatory bodies, like the Central Consumer Protection Authority (CCPA) under Section 10 of The Consumer Protection Act, 2019. Though, The Consumer Protection Act, 2019 doesn't contain explicit provisions as to AI, and consumer protection. But, the vast magnitude of its sections, covers AI-related issues.¹⁴

To rescue, the Indian legal system has started to develop it's AI and customer protection framework. In the case of *National Restaurant Association of India v. Union of India*¹⁵, the

¹¹ Supra note 7

¹² Chander Prabha and Shefali Saluja , *CONSUMER POLICY: THE RELATIONSHIP BETWEEN AI AND DATA PRIVACY* (2024)

¹³ Supra note 1.

¹⁴ Supra note 7

¹⁵ *National Restaurant Association of India v. Union of India*, (2025) SCC OnLine Del 1975

single judge of the Delhi High Court, upheld “The Guidelines to prevent unfair trade practices and protection of consumer interest with regard to levy of service charge in hotels and restaurants” in July 2022, by the CCPA, which was of the view that mandatory collection of service charge by the restaurants is an onerous practice and it constitutes unfair trade practice under Section 2(46) and 2(47) of The Consumer Protection Act, 2019.¹⁶ However, the case doesn’t explicitly state about AI, the principles of transparency and consent, established in this case are relevant for future AI cases.

The United States and the European Union have responded to challenges posed by AI on the privacy of the consumers with a wide ambit of legal regulations. The European Union, through its General Data Protection Regulation, or the GDPR, has set a global benchmark for the protection of data, with stringent rules on privacy, consent and data processing. The GDPR also enshrines the concept of “privacy by design”¹⁷, which mandates the integration of privacy considerations in new technologies, like AI.

The principle of Privacy by design, is particularly relevant in the AI ambit, where there are chances of privacy infringement through various applications. However, the USA has adopted a different approach, then the European Union. The USA has a more fragmented approach, with state level laws like CCPA, providing redressal in cases of harms caused by AI. The CCPA, provides for an approach that is more sector specific, then the European Union that is more of a comprehensive legislation. Due to this diversity in legislations in different jurisdictions, relating to AI and privacy concerns, it becomes a tough task to pursue an uniform international approach, dealing with AI and privacy.¹⁸

4. LEGAL FRAMEWORK IN INDIA

India is now advancing towards the use of digital economy. The usage of AI technology has become omnipresent in every sector, raising serious concerns on consent, privacy and data use. The nine-judge bench of the Hon’ble Supreme Court of India, unanimously has stated in the judgment of *KS Puttaswamy* that a fundamental right to privacy of every individual guaranteed by the Constitution was implicitly afforded, more particularly within Article-21 and Part-III on the whole. The case did not provide a comprehensive AI framework, but it laid the foundation of privacy as a fundamental right. It also means, that a litigant can claim violation of Article 21,

¹⁶ Delhi High Court validates CCPA’s Guidelines which prohibit mandatory levy of a Service Charge by a Restaurant or Hotel <<https://www.khaitanco.com> accessed on 25th November 2025>

¹⁷ Supra note 5

¹⁸ Supra Note 5

if his right to privacy is violated due to AI surveillance mechanisms. The judgment, has further aggravated the need of a comprehensive legislation, that could handle the issue of data protection.¹⁹

India, until recently, did not have a data protection law. The Information Technology Act, 2000, (IT Act) and its associated rules provided certain provisions with regard to data protection. Section-43A of the IT Act provides for civil liability to pay compensation to an individual by compelling a body corporate to pay compensation for failing to implement reasonable security procedures, during, processing or handling of sensitive personal information under its care, if there is wrongful loss to one party and wrongful gain to another. Furthermore Section 72A of provides creates a penalty for the disclosure about any person by any such person who provides service and has access to this information caused by the breach of contract. This covers within its ambit any such person who acts as an intermediary and provides service by virtue of gaining access to the information. Further there is the intent or knowledge that this disclosure causes wrongful gain or wrongful loss without consent, or due to breach of contract. The offender can be penalised up to Rs.25 lakhs for this offence. The term sensitive personal information is defined under Information Technology (Reasonable Security Practices and Procedures And Sensitive Personal Data Or Information) Rules, 2011 under Rule 3 wherein sensitive personal data or information includes: Password, Financial data, health or medical data or data collected or provided in law in relation to any service that involves interaction with a body corporate on a lawful contract basis. However, it shall not include data that is or has been made publicly available, or data provided under RTI Act.

The former structure of data protection in India was found to be highly deficient compared to other countries in the world. It was also noteworthy that several forms of data were not included in Rule 3. Even though the IT Act provides an outline for a safe and lawful handling of data, it essentially confers very limited protection to data in India.²⁰ Therefore, to bring data protection in India at par with other countries of the world.

India now has its first law on data protection in the form of Digital Personal Data Protection Act, 2023 (DPDP Act). The preamble of the Act states that it is an Act to provide that any digital personal data is processed in such a manner that balances the right of the individual to

¹⁹ D. MAJUMDAR AND H.K. CHATTOPADHYAY, Emergence of AI and its implication towards data privacy: From Indian legal perspective, (2020) IJLMH 1

²⁰ Arokia Sushma Dr. Ranjit Oommen Abraham, Dr. R. Haritha Dev ARTIFICIAL INTELLIGENCE AND DATA PRIVACY CHALLENGES: A LEGAL PERSPECTIVE, Indian Journal of Integrated Research in Law Volume V Issue V | ISSN: 2583-0538, 221

protection of data, with a need to process data in a lawful and proper manner. The Digital Personal Data Protection Act, 2023 was passed by the parliament on August 11, 2023 and was then published in the gazette. The Act models itself on the EU'S General Data Protection Regulation, incorporating principles like consent, transparency, data minimisation. The Data controllers must process data securely and implement security standards. The DPDP Act also, just like the GDPR applies extraterritorially.

The DPDP Act establishes a consent-oriented approach²¹, i.e., it requires specific, informed and unconditional consent. Under the Digital Personal Data Protection (DPDP) Act, 2023 of India, lawful consent is the foundation of dispensation private data. Section 6 of the Act clearly dictates that consent must be free, specific, informed, unconditional, and unambiguous with a clear affirmative action. This is a significant move from the blanket or forced consent models often seen in the past. Consent must be granular and restricted to the precise purpose for which the data is required. It cannot be a vague, catch-all agreement. For instance, A data fiduciary must clearly stipulate why they need the data. If the purpose changes, they must obtain fresh consent. The more prominent and desirable change is that a user cannot be asked to agree to "all future uses" or combine multiple distinct purposes into one "I Agree" button.

However, there still remains some gaps that exist in the DPDP Act, Firstly, the Act only applies to personal data in digital form, and not to offline data, or non-personal data. Secondly, since the rules are still in the stage of formation, the law isn't fully functional. And thirdly, the DPDP Act, 2023 doesn't specifically address AI-related issues. Further, The Act enables the government to exempt any of its agencies from application of the Act on certain grounds which renders the Act to be used for state surveillance and resulting into lesser or no liability in case or government data breachers. The DPDP Act, provides for a general framework for data protection, but the need for a AI specific legislation to meet future challenges still remains unrealised.²²

5. INFLUENCE OF AI ON CONSUMER PROTECTION IN INDIA

The Consumer Protection Act primarily deals with safeguarding the rights and duties of the consumers in the marketplace. With the recent technological advancements, and with the growing use of AI in handling consumer information, serious concerns of privacy and fraudulent acts are rising. The rapid growth of technology poses significant challenges to protect personal data and to maintain information security.

²¹ Supra note 20.

²² Id.

The Consumer Protection Act, 2019 (CPA, 2019), does provide a comprehensive approach to tackle with issues relating to goods and services that are enabled by AI. Section 2(16) of the CPA, 2019, defines e-commerce as “*buying or selling of goods or services including digital products over digital or electronic network.*”²³ Though not specifically provided under the Act, if any person faces any defect in digital goods or services, the consumer has the right to take recourse of the Act. The Act, doesn’t explicitly mention the terms like personal data, automated decision making, profiling, automated decision making etc. The Consumer Protection Act, 2019 isn’t a well-equipped legislation, and can’t be fully relied on, to deal with the issues pertaining to AI.²⁴ In India, for a robust protection of consumer privacy from AI-related harms, there is a need of more AI-specific laws, that complement the present data protection regime in India.

6. LEGAL FRAMEWORK IN USA & EUROPEAN UNION

A. Legal Framework in the USA-CCPA, 2018

The California Consumer Protection Act, 2018 (hereinafter referred as CCPA, 2018) gives consumers additional rights about the information that the business collects from them. Entering operation in 2018, the CCPA gives significant control over personal data to the residents of the California. The CCPA regulation provides for the procedure to implement the law.²⁵ The law secures the consumers with new privacy laws, including-

- The right to be informed about the purpose for which the personal data is collected, and for the reasons for which the businesses may use it.
- The right to deletion of personal consumer data, collected, but subjected to some exceptions.
- The right to withdraw from the sale or transfer of personal information.
- The right to the free and indiscriminate use of CCPA rights.

One of the notable aspects of this Act is, that it focuses on data monetization. Organisations should inform the consumer whether they sell out their data and also give an option to the

²³ Consumer Protection Act, 2019

²⁴ Supra note 1

²⁵ California Consumer Protection Act, 2018

consumers to opt-out.²⁶ In November 2020 the CCPA, 2018 was amended by The Consumer Privacy Rights Act, 2023 that added additional privacy provisions. In addition to above, the consumers have also been given additional rights-

- The right to request the businesses to correct any incorrect information they hold about them.
- The right to restrict or limit the disclosure of sensitive or personal information.

Hence, the CCPA, 2018 doesn't contain any AI-specific provisions, but the amendment made by the CPRA, 2023 introduced limited changes like automated decision making and profiling.

B. Legal Framework in the EU- GDPR And EU AI Act,2024

GDPR has set up a benchmark for developing various other statutes of the world, that are based on data privacy. The GDPR is regarded to represent the gold standard for data privacy frameworks, due to its extensive approach of handling personal information. The GDPR focuses on three core principles, i.e., transparency, accountability and users' empowerment.²⁷ Building upon the European Convention on Human Rights, 1950, right to privacy was considered an important right in 1950. With the progress of internet, the need of modern protections was recognised by the European Union. In the year 1995, EU enacted The European Data Protection Directive, which set minimum security and privacy standards on member states implementing the law.

But in 2011, when a Google user sued the company for scanning their mails, a need was felt for a more comprehensive legislation on the 1995 directive. The General Data Protection Regulation (GDPR) was introduced in 2018, to overcome this difficulty. It is meant for the protection of fundamental rights of natural persons with regard to handing out of data.²⁸ The adoption of precautions and measures in the protection of data, as well as guarantee the safe processing of data and notification of breaches if any is now the mandate of GDPR as well. It is expected that the requirement of adoption of precautions and measures for the safe processing of data shall continue to rise in the future; The organisations are instructed to adhere to the

²⁶ Geraldine O Mbah , Data privacy in the era of AI: Navigating regulatory landscapes for global businesses (International Journal of Science and Research Archive, (2024), 13(02), International Journal of Science and Research Archive) 2040–2058

²⁷ Ibid note 32.

²⁸ What is GDPR, the EU's new data protection law? <<https://gdpr.eu/> Accessed on 25th November 2025)

directive in order to protect the rights and sovereignty of natural persons with regards to regards to data processing.²⁹

The GDPR is considered one of the strictest privacy and security law in the world. Formed and drafted for the European Union (or the EU), this regulation has an extraterritorial application, i.e., it imposes obligations on organisations situated anywhere in the world, provided they target and collect data from the people of EU. The GDPR, came into effect on May 25, 2018. GDPR levies heavy fines, against the non-compliance with privacy and security standards.³⁰

C. Key Principles of EU GDPR

Consent - The GDPR requires explicit, and an informed consent from the user, before processing the data. Such consent must be revocable. Organisations must clearly indicate the purpose for which the data collected is used and should also give option to user to withdraw their consent at any time.

Data minimisation - This principle means, that only that much of data must be collected from the consumers that is necessary to accomplish a particular purpose. Extensive data collection from the consumer isn't allowed, hence safeguarding the privacy of the consumers.

Right to be forgotten - This principle allows the user to get their information deleted, when their personal information is either not in use, or the consent given by the consumer has been withdrawn.³¹

Article 1 of the GDPR provides the subject matter and the objectives, which provides for the rules pertaining to the protection of the natural persons in respect of processing personal data, while maintaining full and free movement of such data. These rules ensure the protection of fundamental rights and freedoms of the individuals, especially with regard to their personal data protection rights, while ensuring that the free flow of information is not hampered or prohibited for the reason concerning the protection of individuals with regard to processing of data. GDPR also defines various terms like, personal data, data processing, data subject etc, under Article 4.

Chapter 2 (Articles 5-11) states the various principles of data protection, on which GDPR is based. Article-5 of the GDPR provides for the principle of data processing. The data should be

²⁹ White paper on General Data Protection Regulation (GDPR) <https://ecb.com/en/whitepaper/general-data-protection-regulation-gdpr>.

³⁰ Ibid note 35

³¹ Ibid note 35

processed according to law. The data should also be processed and handled fairly and transparently. Furthermore, personal data should be processed for specific and clear purposes. The data will also have restricted processing and should be relevant for the objective. The data should also adhere to data minimisation principle. The data should also be correctly maintained. The data must be stored in such a way that confidentiality, security and integrity of the data is preserved.

Article 6 states the principle relating to lawfulness of processing of data. The consumer has to give a specific, and an unambiguous consent as to the use of data. Art-6 states the instances wherein it is considered to be legal to process personal data. Personal data may be processed in certain circumstances when it is deemed to be lawful. Such situation may arise when the processing of information becomes necessary in fulfilment of a contract where the data subject is a party, or when it becomes necessary for the data controller to comply with a particular legal requirement. Also relevant in this case may be a situation, where it becomes necessary for the protection of person's vital interests, or when processing becomes a matter of public interests.

Article 7 and 8, tells about consent of the data user. The consent must be given freely, unambiguous, specific and clear. Request of consent must be made in a plain and clear language, and such request must be distinguishable from other matters. Data users have the power to withdraw the consent at any time. Article 8 speaks that children under the age of 13 can only give consent with the permission of their parent. Documentary evidences must be retained for such consent. Article 9, 10 and 11 states the processing of information in specific type of offence, like in criminal convictions etc.

The EU AI Act, 2024 is the most comprehensive legal framework setting out harmonised rules for the use of AI in the EU. It was published in the official journal of the EU on 12th July 2024, after nearly three years of negotiation. It came into effect from 1st August 2024. The enforcement timeline of the EU AI Act is gradual, with most provisions coming will come into application on 2nd August 2026. The EU AI Act represents a wide-reaching framework, that is applicable throughout the European union, in an effort to establish that the legal systems are "safe, transparent, traceable, non-discriminatory, and environment- friendly." The Act introduces a risk-based approach, whereby AI systems are categorised according to potential impact on citizen's rights and safety. This path-breaking legislation thus has set up a blueprint for AI governance.³²

³² Ibid note 40

7. COMPARATIVE PERSPECTIVES

The current legal regime in India, governing data protection is Digital Privacy Data Protection Act, 2023 (commonly known as DPDP Act, 2023). The Act lays down the basic conditions for data protection, i.e. lawful processing, purpose limitation and data minimisation. The DPDP Act lays down general standards of data protection, establishing a ground framework, but its implementation for AI-specific risk is limited. The California Consumer Protection Act, 2018 (hereinafter referred as CCPA, 2018), (implemented in USA) gives consumers additional rights about the information that the business collects from them. Entering operation in 2018, the CCPA gives significant control over personal data to the residents of the California. The CCPA regulation provides for the procedure to implement the law.

GDPR (implemented in EU) has set up a benchmark for developing various other statutes of the world, that are based on data privacy. The GDPR is viewed to represent the gold standard for data privacy frameworks, due to its extensive approach of handling personal information. The GDPR focuses on three core principles, i.e., transparency, accountability and users' empowerment. The following table represents a brief picture of the Comparative position of governing framework in these three potential jurisdictions-

BASIS	INDIA	USA	EU
Legal framework	Digital Personal Data Protection Act, (DPDP Act), 2023	No federal Law, but state law ,i.e. CCPA enforced	General Data Protection Regulation and EU AI Act (2024)
Scope and Coverage	It covers all digital personal data collected from government and private entities.	No universal coverage, sectoral coverage only	Wide scope, applies to all personal data,i.e., collected from digital or non-digital means.
Consumer Rights related to data	• Right to access • Right to redressal of grievances • Right to	• Right to access • Right to deletion • Right to opt out of sale or	Provides strongest rights to the customers, like, right to access, right to deletion, rectification etc.

	withdraw consent	sharing of data.	
Automated decision making (ADM)	No provision for ADM	No general federal ADM Law, limited protection in some states	Article 22 of GDPR penalises ADM
AI-specific Law	India till date has no AI- specific law.	No federal AI law	EU AI act is the first comprehensive AI law.
Regulators	Data Protection Board of India	Multiple agencies and state authorities	Independent data protection authorities in each member state
Penalties	High penalties for noncompliance under the DPDP Act	Penalty varies state wise.	GDPR imposes the highest penalties in the world.

8. CONCLUSION

The widespread use of AI in consumer-oriented industries has resulted in considerable changes in the way personal information is collected, processed, and used. While these innovations come with gains in convenience and efficiency, they also bring pressing concerns regarding data privacy, informed consent, algorithm fairness and individual autonomy. In the Indian context, the legal framework for Data protection is still developing. The Digital Personal Data Protection Act, 2023, is the initial step towards developing a comprehensive regulation. Nevertheless, this legislation doesn't reflect upon the implication of AI in consumer data processing. Similarly, the Consumer Protection Act, 2019, is limited in its authority to respond to the issues created through automated profiling and automated decision making.

This regulatory gap has left consumers exposed to possible data misuses and without any adequate avenues of redressal in case of AI related harm. Limited public understanding and lack of transparency with regard to AI systems has further aggravated these issues. India, USA and European Union take different legal approaches to deal with data protection and AI use in

consumer data. India has a privacy law, Digital Personal Data Protection Act, 2023, but this act doesn't contain AI- specific provisions. The USA has no single specific AI, or, privacy laws, but only a set of state-based laws like The California Consumer Protection Act, 2018 which accounts for an uneven state law. European Union offers the strongest law for AI regulation and data governance, with laws like GDPR And the EU AI ACT, 2024. There is a difficult road lying ahead for the policy makers to realise then to address the concerns highlighted above. Data privacy is something so intrinsically attached with our individuality that can never be compromised on any grounds. The concept of consent has also been expanded to such an extent that without any further delay the urgency requires either a new mechanism to be created to handle AI driven privacy challenges or the existing framework needs to be enabled to be robust enough to contain the dilemma ahead.