EFFECT OF DATA PRIVACY LAWS ON AI

Diksha Taneja[1], Priya Jain[2], VVB Singh[3], Sharwani Pandey[4], Rahul Singh[5]

ABSTRACT

The integration of artificial intelligence (AI) into all facets of contemporary existence has sparked apprehensions over its influence on the confidentiality of data. Although AI has the ability to greatly transform companies and make procedures more efficient, it also presents concerns to personal privacy owing to the enormous processing of data. This study examines the point where AI and data privacy collide, emphasising the need of protecting people' privacy rights in the age of AI. The implementation of DPDPA in India in 2023 is a significant milestone in resolving these concerns and overseeing data processing operations. The DPDPA empowers people to have more authority over their personal data, while also ensuring that organisations are responsible for adhering to data privacy regulations. This article explores the significance of artificial intelligence (AI) and data privacy in the contemporary day, with a focus on the widespread use of AI technology, the changing legal environment, and the ethical concerns related to safeguarding personal information. This text explores the difficulties presented by artificial intelligence (AI) in terms of gathering data, the presence of biased algorithms, and breaches of privacy. It also discusses the legislative framework that governed AI and data privacy in India before the DPDPA was enacted. In addition, the study examines the main provisions of the DPDPA and their consequences for data principals, data fiduciaries, and consent managers. The statement emphasises the significance of collaborating with stakeholders, investing in AI ethics and governance frameworks, and using privacy-enhancing technology. These measures are crucial for complying with data protection rules and promoting innovation in AI-driven applications. Ultimately, this study emphasises the crucial need to maintain a harmonious equilibrium between innovation and safeguarding privacy in the era of artificial intelligence. To manage the difficulties of AI-driven data processing and maintain people' data privacy rights,

[1] Teaching Associate, Faculty of Juridical Sciences , Rama University, Kanpur, U.P, India
[2] Assistant Professor, Faculty of Juridical Sciences , Rama University, Kanpur, U.P, India
[3] Associate Professor, Faculty of Juridical Sciences , Rama University, Kanpur, U.P, India
[4] Teaching Associate, Faculty of Juridical Sciences , Rama University, Kanpur, U.P, India
[5] Assistant Professor, Faculty of Juridical Sciences , Rama University, Kanpur, U.P, India

organisations may solve the problems provided by AI and use legislative frameworks such as the DPDPA.

Keywords: AI, data, privacy, DPDPA, National AI Strategy.

INTRODUCTION

Artificial intelligence (AI) has become a crucial component of our everyday existence, altering the manner in which we engage in work, interact, and derive amusement. AI is omnipresent, from Siri and Alexa to tailored suggestions on Netflix. Nevertheless, as artificial intelligence becomes more widespread, it is essential to contemplate the influence it has on our privacy.[6]Artificial intelligence algorithms are educated using extensive quantities of personal data, which may be used to generate forecasts and make determinations on individuals. This jeopardises our privacy in ways that were previously inconceivable. The topics of AI and data privacy are intricate and interconnected matters that provide both possible advantages and disadvantages. AI has the capacity to significantly boost many sectors, optimise decision-making, and simplify operations. However, AI systems have the capability to handle and examine vast quantities of personal data, which may raise issues about privacy if the data is exploited or inadequately safeguarded. Data privacy encompasses the safeguarding of personal data and the entitlement of people to govern the collection, use, and dissemination of their personal information. Data privacy is crucial in the AI-driven era, since AI systems handle and analyse extensive volumes of personal data, enabling the discovery of previously unidentified patterns and insights. Nevertheless, this also implies that personal information is more susceptible to being exploited or mismanaged. Data privacy regulations such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are designed to empower people to have authority over their personal data and to guarantee the appropriate safeguarding of personal information. On August 11, 2023, the President of India approved the Digital Personal Data Protection Act (DPDPA), which has now been officially recognised as a law following its publication in the Official Gazette.Though not yet implemented this law is expected to impact

[6] "Explained: How AI is changing our everyday life", The Times of India (18 October, 2023) https://timesofindia.indiatimes.com/education/learning-with-toi/explained-how-ai-is-changing-our-everyday-life/articleshow/103930505.cms (Last accessed on March 18, 2024).

the intersection between AI and date privacy and hence the same shall be discussed extensively hereby.[7]

RELEVANCE OF AI AND DATA PRIVACY IN MODERN ERA

In today's modern era, the relevance of AI and data privacy cannot be overstated. Here's why:[8]

1. Proliferation of AI: Technologies that are powered by artificial intelligence are progressively being incorporated into a variety of facets of day-to-day living, ranging from personalised suggestions on streaming platforms to autonomous cars and healthcare diagnostics. The quantity of data that is being gathered, analysed, and used is likewise growing at an exponential rate as artificial intelligence becomes more widespread. This increased dependence on artificial intelligence highlights the essential need of preserving the privacy rights of persons and ensuring that personal data is handled in a responsible and ethical manner via the use of AI.
2. Data as a Currency: As a result of the advent of the digital era, data has become a valuable currency that is fueling innovation, economic development, and competitive advantage for companies and organisations. When it comes to privacy, however, this greater dependence on data comes with its own set of inherent concerns. It is common for artificial intelligence systems to need access to sensitive personal information in order to train and develop their algorithms. These systems depend on large volumes of data. As a consequence of this, issues over data privacy have emerged as a key topic of debate in the context of artificial intelligence research, legislation, and implementation.
3. Ethical Considerations: The ethical concerns that are associated with the protection of personal information have been at the forefront of public conversation as artificial intelligence technologies continue to improve. In the context of concerns about the

[7] Aiman J. Chishti, "President Gives Assent To Digital Personal Data Protection Act 2023", LiveLaw (12 Aug 2023) https://www.livelaw.in/top-stories/president-gives-assent-to-data-personal-data-protection-act-235056

[8] Karl Manheim and Lyric Kaplan, "Artificial Intelligence: Risks to Privacy and Democracy", 21 Yale J.L. & Tech. 106 (2019).

appropriate use of artificial intelligence and the preservation of people' privacy rights, questions of permission, transparency, algorithmic bias, and accountability are at the centre of conversation. The ethical implications of AI-driven decision-making, as well as the possibility of prejudice or injury, further emphasise the need of implementing stringent protections for data privacy.

4. Regulatory Landscape: Regulations regarding data privacy are being enacted by governments all over the globe in order to safeguard the rights of people and ensure that organisations are held responsible for the manner in which they handle personal information. A precedent for privacy laws on a worldwide scale has been established by regulations such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. It is necessary for organisations that deploy artificial intelligence systems to comply with these standards in order to guarantee that the systems conform to the principles of data minimization, purpose restriction, and transparency at all times.
5. Trust and Reputation: The upkeep of trust and reputation is of the utmost importance for companies and organisations that use artificial intelligence technology. The confidence of consumers, partners, and stakeholders may be damaged when there are instances of data breaches, privacy violations, or unethical use of personal data. This can result in reputational damage as well as financial ramifications. Putting an emphasis on data privacy and implementing best practices for responsible data stewardship are two ways that organisations may assist in establishing and sustaining trust in a world that is becoming more data-driven.

CHALLENGES PERTAINING TO AI AND DATA PRIVACY

Data privacy faces several challenges in the context of AI:[9]

1. Data Collection and Storage: For artificial intelligence systems to be able to properly train and make correct predictions or choices, they often need access to large volumes of data. A variety of personal information, including demographics, interests, behaviours, and even biometric data, may be included in this assortment of data. Nevertheless, the gathering and storage of such data might provide considerable threats to individuals' privacy, particularly in the event that appropriate controls are

[9] Supra note 3.

not in place. Concerns regarding unauthorised access, abuse, or exploitation of an individual's personal data may arise as a result of the fact that individuals may be ignorant of the comprehensiveness of data gathering or the manner in which their information is being used.

2. Data Breaches: Artificial intelligence systems are not immune to the vulnerabilities that may be caused by data breaches, which pose a significant risk to the privacy of data. Artificial intelligence (AI) systems have the potential to become targets for hostile actors who are looking to get unauthorised access to sensitive data if they are not appropriately protected. A breach of an artificial intelligence system might lead to the revelation of personal information, financial data, or other private information, which would have significant repercussions for both persons and organisations.
3. Algorithmic Bias: There is a widespread problem of bias in artificial intelligence algorithms, which may have significant repercussions for the fairness and privacy of data. Using the data they are educated on, artificial intelligence systems are able to recognise patterns and make predictions. On the other hand, if the training data includes prejudices or reflects historical injustices, then the AI models may continue to perpetuate or even aggravate these biases. It is possible for this to result in discriminatory consequences, such as the unjust denial of opportunities or services to certain persons or groups on the basis of their race, gender, or other protected characteristics. It is essential to address algorithmic bias in order to guarantee that artificial intelligence systems will respect the privacy of persons and adhere to the values of justice and equality.
4. Inference of Sensitive Information: Artificial intelligence presents a number of unique issues, one of which is its capacity to infer sensitive information from data pieces that seem to be harmless. Artificial intelligence systems are able to analyse patterns and create predictions about specific persons' behaviours, preferences, health state, and other personal characteristics, even if the individuals in question do not divulge some information directly. Consequently, this gives rise to worries over the deterioration of privacy as well as the possibility of intrusive monitoring or profiling methods. As an instance, artificial intelligence systems that are used in targeted advertising or recommendation engines may collect a substantial amount of data on the online activities of people and then use this information to infer personal preferences or traits, perhaps without the individuals' knowledge or agreement.

LAWS GOVERNING AI AND DATA PRIVACY: PRE DPDPA ERA

Before the Digital Personal Data Protection Act (DPDPA) of 2023, India's legal landscape concerning Artificial Intelligence (AI) lacked comprehensive and explicit regulation. However, several existing laws indirectly addressed aspects relevant to AI, often intersecting with concerns regarding data privacy and security.[10]

1. Information Technology Act, 2000: This fundamental piece of law is largely concerned with electronic governance and cybersecurity for the most part. Despite the fact that it does not specifically reference artificial intelligence, it does include a number of provisions that are relevant to the operations of AI systems, notably those that pertain to data protection and cybersecurity. As an example, Sections 43A and 72A[11] are concerned with the protection of sensitive personal data and, correspondingly, establish penalties for the dissemination of information without authorization. In the context of artificial intelligence systems, which often entail the processing of personal data, these clauses are crucial because they underline the need of developing measures to protect data privacy.
2. Indian Contract Act, 1872: The Indian Contract Act, 1872 is the primary legislation governing the principles and regulations of contract law within India. It is imperative to note that the Act was enacted prior to the advent of Artificial Intelligence (AI) and its subsequent implications on contractual relationships. Notwithstanding its antiquity, this Act continues to possess significant pertinence within the realm of AI applications, primarily attributable to the complex contractual associations that underlie AI development, implementation, and utilisation.Within the domain of artificial intelligence, contractual agreements hold significant importance as they serve to coordinate and regulate the cooperative endeavours of multiple parties, including developers, data providers, and end-users. The aforementioned contracts serve to clearly outline and define the rights, obligations, and responsibilities of all parties involved. For example, it is common for agreements entered into by artificial intelligence developers and their clients to include provisions that specify the extent of the work to be performed, the items to be delivered, the schedule to be followed,

[10] Praveen Kumar Mishra, “AI And The Legal Landscape: Embracing Innovation, Addressing Challenges”, LiveLaw (27 Feb 2024) https://www.livelaw.in/lawschool/articles/law-and-ai-ai-powered-tools-general-data-protection-regulation-250673 (Last accessed on March 17, 2024).

[11] The Information Technology Act, 2000.

and the terms governing payment. Furthermore, it is important to note that in the current discourse, data privacy holds significant importance. Consequently, contractual agreements that govern projects involving artificial intelligence commonly include strong provisions that specifically address concerns related to data privacy and confidentiality.[12]

3. Consumer Protection Act, 2019: The Act is primarily intended to protect and uphold the rights and interests of consumers. Although the law in question does not explicitly mention artificial intelligence (AI), it is applicable to any transactions that involve products or services driven by AI. Under the provisions of this law, consumers have the right to seek redress in instances where AI-powered products fail to meet their expectations or infringe upon data privacy norms.[13]
4. Intellectual Property Laws: India's intellectual property laws, namely the Patents Act, Copyright Act, and Trademarks Act, provide legal safeguards for a range of intellectual property rights that are pertinent to the field of artificial intelligence (AI), encompassing algorithms, software, and AI-generated content. While primarily focusing on the protection of intellectual property, these laws indirectly impact the development and innovation of artificial intelligence, which may necessitate the examination of data privacy concerns.[14]
5. Draft National AI Strategy: A National Artificial Intelligence Strategy was being developed by India prior to the DPDPA to provide guidance for the development and deployment of AI. This strategy document delineated principles, policies, and initiatives pertaining to AI governance, research, and innovation, albeit without legal enforceability. The significance of data privacy as a fundamental component of AI governance was presumably underscored, along with the necessity for forthcoming regulatory frameworks to effectively tackle privacy apprehensions.[15]

THEDIGITAL PERSONAL DATA PROTECTION ACT (DPDPA) 2023

The Digital Personal Data Protection Act (DPDPA), enacted in India as of August 11, 2023, introduces several provisions aimed at regulating the processing of personal data and

[12] Supra note 5.
[13] Supra note 5.
[14] Supra note 5.
[15] Available at: https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf (Last accessed on March 20, 2024).

safeguarding individuals' privacy rights.Section 2 of the Act defines key stakeholders involved in data processing, including Data Principals, Consent Managers, the Data Protection Board (DPB), Data Processors, Data Fiduciaries, and Significant Data Fiduciaries. This delineation of roles lays the foundation for accountability and responsibility in data processing activities.Sections 11-14 outline the data protection rights granted to Data Principals, including the right to access personal data, correction, completion, updating, erasure, grievance redressal, and the right to nominate representatives for exercising data protection rights. These rights empower individuals to control their personal data and hold Data Fiduciaries accountable.Section 5 enumerates circumstances where processing personal data is deemed legitimate, such as fulfilling legal obligations, government schemes, and voluntary consent. Clarity in lawful data processing activities provides guidance for organizations and individuals regarding acceptable data use cases. However, the Act presents challenges and policy dilemmas. Section 3 exempts publicly available data from certain provisions, deviating from global standards. Section 7 grants unilateral powers to the government for data flow restrictions, posing challenges in international data transfers. Additionally, exemptions for startups raise questions about privacy-compliant ecosystems, while focusing on Data Fiduciaries' duties over Data Processors' obligations may impact accountability.Furthermore, the Act introduces Consent Managers as entities managing consent processes. Section 5(7)-(9) outlines their roles and responsibilities. AI integration offers potential benefits, such as automating consent management processes, providing personalized consent experiences, ensuring transparency, accountability, and supporting grievance redressal processes. However, challenges remain in clarifying AI's role and addressing accountability issues.[16]

ROLE OF AI USAGE IN SHAPING RIGHTS OF DATA PRINCIPALS

Within the realm of AI applications, specifically those that utilise generative AI technologies, it is imperative to acknowledge the significance of the provisions delineated in Sections 11 to 14 of DPDP Act in upholding the fundamental rights of individuals, commonly referred to as data principals. As per the provisions outlined in Section 11, it is important to note that data principals are granted the inherent and essential entitlement to obtain access to pertinent information pertaining to the processing of their personal data by a data fiduciary. The aforementioned right to information holds utmost significance in facilitating data principals'

[16] Ashutosh Kumar, "Artificial Intelligence and Law in India", 8 JETIR 539-544 (2021).

understanding of the manner in which their data is employed within artificial intelligence applications. It is our contention that this particular system grants individuals the authority to exercise their right to make well-informed determinations with respect to the consent they furnish for the processing of their data. Furthermore, within the framework of AI acting as consent managers, it is crucial to thoroughly examine the complexities of how technology enhances consent management, in order to achieve a comprehensive comprehension of data processing dynamics. Going forward, it is important to note that pursuant to Section 12, data principals are afforded the right to rectify any inaccuracies or incompleteness that may exist in their personal data. Within the purview of AI applications, wherein algorithms render determinations predicated upon voluminous datasets, the spectre of fallibility in data processing assumes considerable magnitude. The aforementioned errors, if left unaddressed, may potentially result in significant and far-reaching ramifications, including but not limited to the unjustified denial of essential services or the dispensation of inequitable treatment. Therefore, it is crucial to acknowledge the utmost significance of the provision for data correction in order to effectively mitigate said risks and uphold the rights of data principals. Moreover, it is important to note that Section 13 explicitly guarantees that data principals are provided with accessible channels through which they can seek redressal for any grievances they may have. Considering the intricate nature of AI applications and the possibility of obscure data processing mechanisms, it is of utmost importance to establish sturdy mechanisms by which individuals can pursue remedies for infringements upon their privacy rights. The aforementioned provision serves to emphasise the imperative of transparency and accountability in the context of data processing activities driven by artificial intelligence.[17]

Furthermore, it should be noted that pursuant to Section 14, data principals are granted the authority to designate representatives who shall be responsible for the exercise of their rights as provided for in the aforementioned legislation. The aforementioned provision assumes particular significance in situations wherein artificial intelligence undertakes the processing of data on behalf of individuals who, due to their status as minors or individuals with disabilities, may lack the capacity to assert their own interests. By virtue of its provisions, the DPDP Act effectively facilitates the authorization of representatives, thereby guaranteeing

[17] Zhao, J., Gómez Fariñas, B. Artificial Intelligence and Sustainable Decisions.Eur Bus Org Law Rev 24, 1–39 (2023).https://doi.org/10.1007/s40804-022-00262-2

the sufficient safeguarding of the rights of marginalised and susceptible collectives within the realm of AI-facilitated data processing endeavours.

Furthermore, it is imperative for data fiduciaries who employ generative AI applications to establish and enforce stringent measures aimed at safeguarding the privacy of data principals, in addition to complying with the aforementioned statutory provisions. The aforementioned measures may encompass rigorous access controls, anonymization methodologies, ongoing surveillance for biases and discriminatory patterns, and all-encompassing educational initiatives designed to augment data principals' understanding of their privacy rights. Through the implementation of these proactive measures, data fiduciaries have the ability to mitigate the inherent risks that are associated with generative AI applications and, in doing so, uphold the fundamental principles of data privacy and protection within a world that is becoming increasingly driven by artificial intelligence.

SUGGESTIONS

- Organisations should have strong methods to continuously monitor AI systems and data processing operations in order to guarantee compliance with data privacy rules, such as the DPDPA. Periodic audits and evaluations should be carried out to detect and rectify any possible privacy issues or infringements.
- Increased investment in AI ethics and governance frameworks is necessary to tackle ethical challenges related to AI-driven data processing. It is crucial for organisations to give priority to openness, fairness, and accountability in AI systems in order to reduce the dangers associated with algorithmic bias and privacy breaches.
- It is essential to provide comprehensive education and awareness programmes to stakeholders, such as data principals, data fiduciaries, and consent managers, in order to improve their comprehension of data privacy rights and obligations. Training courses and workshops may assist stakeholders in understanding and navigating the intricacies of data privacy regulations, therefore ensuring adherence to legal mandates.
- The successful implementation and enforcement of data privacy legislation requires the collaboration of government agencies, industry parties, and civil society organisations. Knowledge sharing platforms and forums may enhance the dissemination of optimal methods and insights gained in the domain of artificial intelligence and data privacy.

- Organisations should consider using privacy-enhancing technologies, such as differential privacy, homomorphic encryption, and federated learning, to safeguard sensitive personal data while optimising the effectiveness of AI systems. These technologies may assist organisations in attaining a harmonious equilibrium between safeguarding data privacy and fostering innovation in applications powered by artificial intelligence.

CONCLUSION

In conclusion, AI and data privacy bring both potential and difficulties in today's digital world. AI might transform businesses and enhance decision-making, but data privacy and security are major issues. Indian lawmakers passed the DPDPA to solve these issues and protect privacy. The DPDPA gives data principals more control over their personal data and holds data fiduciaries responsible for data privacy compliance. Government agencies, industry players, and civil society organisations must work together to execute the DPDPA. Organisations must prioritise ethics, invest in AI ethics and governance frameworks, and increase stakeholder education and awareness to manage AI-driven data processing while protecting data privacy. Organisations should combine innovation and privacy in the AI age by taking a proactive approach to data privacy and using privacy-enhancing technology.

REFERENCES

PRIMARY SOURCES

- The Indian Contract Act, 1872.
- The Information Technology Act, 2000.
- The Consumer Protection Act, 2019.
- The Digital Personal Data Protection Act, 2023.
- The National Artificial Intelligence Strategy.

SECONDARY SOURCES

- “Explained: How AI is changing our everyday life”, The Times of India (18 October, 2023) https://timesofindia.indiatimes.com/education/learning-with-toi/explained-how-ai-is-changing-our-everyday-life/articleshow/103930505.cms (Last accessed on March 18, 2024).
- Aiman J. Chishti, “President Gives Assent To Digital Personal Data Protection Act 2023”, LiveLaw (12 Aug 2023) https://www.livelaw.in/top-stories/president-gives-assent-to-data-personal-data-protection-act-235056
- Karl Manheim and Lyric Kaplan, “Artificial Intelligence: Risks to Privacy and Democracy”, 21 Yale J.L. & Tech. 106 (2019).

- Praveen Kumar Mishra, "AI And The Legal Landscape: Embracing Innovation, Addressing Challenges", LiveLaw (27 Feb 2024) https://www.livelaw.in/lawschool/articles/law-and-ai-ai-powered-tools-general-data-protection-regulation-250673 (Last accessed on March 17, 2024).
- Ashutosh Kumar, "Artificial Intelligence and Law in India", 8 JETIR 539-544 (2021).
- Zhao, J., Gómez Fariñas, B. Artificial Intelligence and Sustainable Decisions. Eur Bus Org Law Rev 24, 1–39 (2023). https://doi.org/10.1007/s40804-022-00262-2