Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2024 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Navigating the Frontier: AI, Data Privacy and India's Digital Personal Data Protection Act

Arya Gupta[a]

[a]Department of Law, Rani Durgavati Vishwavidyalaya, Jabalpur, India

Received 21 June 2024; *Accepted* 24 July 2024; *Published* 29 July 2024

The advent of the technology of Artificial Intelligence has significantly contributed to the comforts of human life. However, the rapid integration of AI into various sectors has raised certain questions regarding its universal applicability and safety, leading to discussions on ethics and legal frameworks surrounding AI. In today's world, AI is seen as a catalyst for economic advancement and overall progress. But, at the same time, the integration of AI into cyberspace has raised significant privacy issues and contributed to an increase in cybercrimes. In India, the breach of crucial personal data and violations of privacy rights is a fundamental issue that has raised concerns among individuals and organizations alike. It is critical to address this problem to ensure the protection of personal data and safeguard the privacy rights of individuals. This article aims to examine the implications of AI and Machine Learning technologies on cyberspace and the right to privacy, in light of the Digital Personal Data Protection Act 2023[1], addressing challenges such as prejudice and discrimination in AI algorithms, transparency and accountability deficits, privacy concerns, and the difficulties faced by the judiciary and law-making bodies considering the rapid evolution of AI technology. It will particularly examine the measures in place to protect privacy and the extent to which the economy relies on AI.

Keywords: *artificial intelligence, data protection, cyberspace, right to privacy, legal framework*

[1] Digital Personal Data Protection Act 2023

INTRODUCTION

The race to become a world leader in the development of AI technologies has only begun. In India, significant amounts of investments have been made by private and public actors in the field. The expenditure on AI and ML technologies by the Indian government has been on a steep upward curve. Recently, the Cabinet approved over Rs. 10,300 crores for the India AI mission. As per NITI Aayog, by 2035, AI has the potential to add 1 trillion dollars to India's economy.[2]

In order to keep pace with the rapid development and deployment of AI as well as to ensure that the personal data of the consumers does not get in jeopardy, we need robust legislations that regulate the use of AI so that it does not infringe upon the right to privacy of a consumer. At first, India employed a hands-off approach concerning AI regulation, however, with the increasing number of cybercrimes associated with AI, thanks to the easy and often free availability of generative AI tools, the need for stricter regulations is now being felt as an urgent necessity.

This article attempts, firstly, to decode the twenty-first century's fourth industrial revolution, i.e. AI and how it uses data to develop itself. Contained within the first part is also an overview of the rapid synergization of Artificial Intelligence technologies and cyberspace and how it is leading to an increase in cybercrimes. Secondly, it seeks to investigate AI's potential to affect privacy rights and the protection of users' personal data. Thirdly, it aims to explore how the Digital Personal Data Protection Act 2023[3] seeks to address the users' privacy concerns specifically those which are associated with the use and misuse of AI technologies. Lastly, it seeks to identify the limitations of DPDPA in dealing with issues involving personal data and the wider sets of cybersecurity problems associated with GenAI technologies. It also seeks to explore the existing and proposed legal frameworks that can facilitate the efficient use of AI technologies without violating core privacy rights.

---

[2] Ministry of Electronics & IT, 'Cabinet Approves Over Rs 10,300 Crore for IndiaAI Mission, Will Empower Ai Startups and Expand Compute Infrastructure Access' (*PIB*, 07 March 2024) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2012375> accessed 19 June 2024

[3] Digital Personal Data Protection Act 2023

WHAT IS ARTIFICIAL INTELLIGENCE?

'Artificial Intelligence' in the broadest sense of the term, is that branch of computer science that is instrumental in developing technologies that mimic human behaviour. 'Artificial intelligence, or AI, is the technology that enables computers and machines to simulate human intelligence and problem-solving capabilities.'[4] 'AI is a machine's ability to perform the cognitive functions we associate with human minds, such as perceiving, reasoning, learning, interacting with the environment, problem-solving, and even exercising creativity.'[5] 'Artificial intelligence algorithms are designed to make decisions, often using real-time data. They are unlike passive machines that are capable only of mechanical or predetermined responses. Using sensors, digital data, or remote inputs, they combine information from a variety of different sources, analyze the material instantly, and act on the insights derived from those data.'[6] Therefore, for instance, if a user chooses to share his personal information on social media platforms, online marketplaces, blogs, websites, video sharing platforms or online gaming platforms, etc., that piece of information shared by the individual on the internet is collected and analyzed by the AI systems and processed by market entities in a way that could potentially abuse this personal data. Moreover, this personal information which could include sensitive information like residential addresses, medical history, financial information, etc., could fall into the hands of malicious actors who could possibly exploit such vulnerabilities leading to cyber frauds and identity thefts.

How does data generated by IoT devices encroach upon the right to privacy of individuals?

Internet of Things (IoT) devices are fairly ubiquitous in today's consumer goods. 'The number of Internet of Things (IoT) devices worldwide is forecast to almost double from 15.9 billion in

[4] 'What is AI (Artificial intelligence)?' (*Mckinsey and Company*, 03 April 2024) <https://www.mckinsey.com/Featured-Insights/Mckinsey-Explainers/What-Is-Ai> accessed 19 June 2024

[5] *Ibid*

[6] Darrell M. West and John R. Allen, 'How artificial intelligence is transforming the world' (*Brookings,* 24 April 2018) <https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/> accessed 19 June 2024

2023 to more than 32.1 billion IoT devices in 2030.'[7] 'IoT technology' at its most basic level can be understood as a technology that establishes a real-time connection between interconnected devices and the internet. Even though IoT has undoubtedly increased connectivity and accessibility of users with their devices, it is important that we do not ignore the associated challenges such as cybersecurity and data privacy. A significant drawback of the IoT is its lack of security procedures comparable to those on servers, personal computers (PCs), and laptops. Most embedded devices lack the computational capabilities to implement sophisticated security rules and encryption protocols effectively.[8] Cyber attackers can target an unsecured IoT device or network, to gain unauthorized access to personally identifiable information (PII) or other confidential user data. The 2024 SonicWall Cyber Threat Report provides that the global volume of IoT Exploits rose by 15%, as connected devices continue to rapidly multiply, bad actors are targeting weak points of entry as potential attack vectors into organizations.[9]

AI is becoming increasingly important in the Internet of Things (IoT) ecosystem because it can help to extract insights from the vast amounts of data generated by connected devices.[10] The learning system of AI is practically useless without 'Big Data' as AI tools like generative AI or predictive AI, rely on it extensively to learn, train, and evolve. And when we say big data, we mean *really* big—with an estimated 2.5 quintillion bytes of data generated each day worldwide, the sheer scale of data available to train artificial intelligence is unprecedented.[11] Additionally, this big data is categorized into structured, unstructured, semi-structured, and streaming data. The structured data comprises organized and labelled information from databases, spreadsheets, ERP, and CRM systems. Unstructured data comprises data of various sorts like

[7] Lionel Sujay Vailshery, 'Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033' (*Satista*, 12 June 2024) <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> accessed 19 June 2024

[8] Tinshu Sasi et. al., 'A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges' (2023) Journal of Information and Intelligence <https://doi.org/10.1016/j.jiixd.2023.12.001> accessed 19 June 2024

[9] '2024 SonicWall Mid-Year Cyber Threat Report' (*SonicWall*) <https://www.sonicwall.com/Threat-Report/> accessed 19 June 2024

[10] 'Artificial Intelligence in IoT: Enhancing Connectivity and Efficiency' (*Device Authority*) <https://deviceauthority.com/Artificial-Intelligence-In-Iot-Enhancing-Connectivity-And-Efficiency/> accessed 19 June 2024

[11] Morgan Sullivan , 'Examining Privacy Risks In AI Systems' (*Transcend Blog,* 01 December 2023) <https://transcend.io/blog/ai-and-privacy> accessed 19 June 2024

social media posts, emails, photos, videos, etc. Semi-structured data is basically unstructured data but with markers and pointers to help with the identification of key factors in the data set. Streaming data refers to the data generated in real-time from IoT devices or from live-streaming on social media, navigation, tracking, etc. which has been stored for later data analysis. At the end of the day, the vast majority of this raw data is useless unless it's fed to a computer system to train predictive models to make future predictions. While the continuous collection of data is instrumental to harnessing AI's machine learning capabilities, it can also lead to the exposure of personal information of individuals. 'Predictive harm' is caused when complex algorithms infer sensitive information from apparently innocuous data. Highly private information like sexual orientation, political views, religious beliefs, financial status, health status, etc. can be predicted by AI tools causing erosion of autonomy by influencing or predicting individual behaviour without their knowledge or consent. Additionally, predictive models can amplify societal biases reflected in the data set they are trained on. This can lead to detrimental consequences for minority communities, for they could, inter alia, get targeted by predictive policing algorithms due to historical biases in crime data. Overall, these emerging privacy risks require thorough legal, ethical, and technological measures to protect privacy in the era of AI.

WHAT IS GENERATIVE AI?

Generative Artificial Intelligence (GenAI) refers to unsupervised and semi-supervised machine learning algorithms that enable computers to generate original content like text, images, music, etc., by training on massive amounts of existing data. GenAI has been the talk of the town ever since the launch of ChatGPT in the year 2022 by the OpenAI. ChatGPT is a large language model capable of understanding and generating natural language and other different types of content to perform wide-ranging tasks.[12] Deep learning has been behind significant GenAI achievements like GPT-4 by OpenAI; Google's Bard; Meta's Llama 2; Anthropic's Claude 2; etc. Deep learning is a subset of machine learning that uses algorithms based on artificial neural networks, modelled after the human brain.[13] Machine learning can either be shallow or deep,

[12] 'What Is Generative Ai?' (*Ibm Research*, 20 April 2023) <https://research.ibm.com/blog/what-is-generative-AI> accessed 19 June 2024
[13] *Ibid*

therefore, if a machine learning algorithm uses only a few layers of data, limiting the amount of data utilized by the AI, it is called shallow learning. On the other hand, when a machine learning algorithm utilizes hundreds of layers it becomes a deep learning network. Huge amounts of data are essential to developing an understanding of highly abstract concepts, necessary for generating strikingly realistic content.[14]

As GenAI develops and becomes more integrated into our daily lives, it raises many concerns regarding data privacy. For instance, 'deep fakes' (by combining deep learning and fake) is a technology that employs a deep learning algorithm called 'Generative Adversarial Networks (GANs)' to alter audio or video to create a false but convincing video of people doing or saying things they never actually did.[15] Another major concern around GenAI is its potential misuse in generating 'spam, fraudulent reviews or even cyberattacks on a large scale.'[16]

REGULATION OF AI AND LARGE LANGUAGE MODELS IN INDIA

According to a report published by NetApp,[17] India ranks at the top in the global implementation of AI projects. The report reveals India as a global leader with seventy per cent of companies having operational or ongoing AI projects. While it is remarkable that India is making significant strides in the field of AI, it is also worth noting that there has been a worldwide 1265% increase in phishing emails, a 967% increase in credential phishing of which 39% of all mobile-based attacks were SMS phishing (Smishing), since the launch of ChatGPT in November 2022, indicating an era of cybercrimes driven by GenAI.[18]

---

[14] Matthew Humerick, 'Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence' (2018) 34(4) Santa Clara High Technology Law Journal <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/> accessed 19 June 2024

[15] 'Deceptive Audio or Visual Media ('Deepfakes') 2024 Legislation' (*NCSL,* 07 May 2024) <https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation> accessed 19 June 2024

[16] Ajay Sudhir Bale et. al., 'The Impact of Generative Content on Individuals Privacy and Ethical Concerns' (2024) 12(1) International Journal of Intelligent Systems and Applications in Engineering <https://ijisae.org/index.php/IJISAE/article/view/3503> accessed 19 June 2024

[17] 'India Ranks Highest For Global Implementation Of Ai Projects: Report' *The Hindu Businessline* (24 April 2024) <https://www.thehindubusinessline.com/info-tech/india-ranks-highest-for-global-implementation-of-ai-projects-report/article68101507.ece> accessed 19 June 2024

[18] 'Slashnext' (*Slashnext,* 30 October 2023) <https://slashnext.com/> accessed 19 June 2024

As AI finds increasing application in our daily lives, the reliance on digital personal data also increases significantly to facilitate AI-driven personalized services. As a result, heightened concerns regarding data privacy and protection have caused the European Union to enact the landmark AI Act[19], which will take effect in June 2024. While India is yet to have a dedicated AI legislation, it does have a data protection legislation titled "Digital Personal Data Protection Act 2023[20]" which was published in the Official Gazette on 11 August 2023, but the exact date of its coming into force is yet to be announced by the government. At present, the Indian Data Protection law is the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[21] (SPDI Rules) until the rules under DPDPA are notified. SPDI rules regulate the processing of Personal Data/ Information and/or Sensitive Personal Data/Information defined as including information relating to passwords, financial information, sexual orientation, biometric information, medical information, physical, physiological, and psychological conditions under the rules, by providing that entities holding SPDI must maintain reasonable specific security standards. GenAI models in India, thus, need to ensure that SPDI does not form a part of the dataset that is used to train the large language model unless explicit consent has been obtained by the individual to whom the SPDI is concerned.

Personal data protection under the Digital Personal Data Protection Act 2023:[22] The DPDPA aims to regulate the processing of individuals' 'personal data'[23] collected in either digital form or non-digital form and then digitized later, from misuse by certain entities, known as 'Data Fiduciaries'[24] under the act. This is unlike the EU's data protection law, GDPR (General Data Protection Regulation) which protects personal data even if it is non-digital. Moreover, the act excludes from its scope personal data that has been made available publicly by the Data Principal or by any other person legally bound to make that data publicly available. 'Personal Data' under the act, is defined as any piece of information that is capable of identifying the

[19] Artificial Intelligence Act 2024
[20] Digital Personal Data Protection Act 2023
[21] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Or Information) Rules 2011
[22] Digital Personal Data Protection Act 2023
[23] Digital Personal Data Protection Act 2023, s 2(U)
[24] Digital Personal Data Protection Act 2023, s 2(I)

person to whom the information relates. The DPDPA further provides that a Data Fiduciary is any person or persons who determine the means and purpose of processing personal data and the person to whom such personal data belongs is referred to as a 'Data Principal' in the Act.

The term 'Personal Data Breach' is broadly defined in the act to include any unauthorized proc essing of personal data, as well as any accidental disclosure, acquisition, sharing, use, alteratio n, destruction, or loss of access to personal data that jeopardizes the confidentiality, integrity, o r availability of such data. Furthermore, the DPDPA does not specifically address AI or GenAI-related concerns, but any cybersecurity incidents involving personal data like an individual's personal photographs and videos available online on social media platforms, or any private information that can be used to identify the person are covered under DPDPA Section 2 (u)[25]. Additionally, DPDPA highlights an individual's right to be informed about the personal data a Data Fiduciary is collecting and the purpose behind this collection. According to section 6 of the Act[26], consent is valid only when it is given duress-free and is specific, informed, unconditional, and unambiguous, involving a clear affirmative action indicating agreement to the processing of personal data for the specified purpose and such processing would be considered legitimate only if it is carried out according to the provisions of the Act and is not for an unlawful purpose.

Data Scraping and DPDPA 2023:[27] Data Scraping also known as web scraping usually involves a computer program or 'bots' collecting vast amounts of data from publicly available and human-readable sources such as websites, social media platforms, public databases, etc. In this digital era, data is the new gold and the internet is a goldmine. AI or GenAI companies collect large amounts of data from the internet and then use it to train their AI models. In 2023, companies using GenAI foundational models saw a slew of lawsuits filed against them challenging the methods adopted by them for obtaining data required for training their AI models, the most famous being the class-action lawsuit filed by the world-renowned authors and publishers against OpenAI and Microsoft in September 2023.[28] In the suit, it was alleged by

[25] Digital Personal Data Protection Act 2023, s 2(U)
[26] Digital Personal Data Protection Act 2023, s 6
[27] Digital Personal Data Protection Act 2023
[28] Satyen K Bordoloi, 'Data Scraping Ai Companies & Writers Fight To Define Future Of Ai' (*Sify*, 8 January 2024) <https://www.sify.com/Ai-Analytics/Data-Scraping-Ai-Companies-Writers-Fight-To-Define-Future-Of-Ai/> accessed 19 June 2024

the plaintiffs that these companies illegally and without the consent of the authors and the publishers used their copyrighted works by scraping their books, journals, and articles from the sources available on the internet to train their AI foundation models. Additionally, they also alleged that their reputation, privacy, and creative control have been violated by these actions and therefore sought a permanent injunction to prevent the defendants from using their works.

Data Scraping is not specifically regulated under the DPDPA since personal data that is publicly available is entirely excluded from the scope of this legislation. This is in stark contrast with the provisions made under the GDPR (General Data Protection Regulation), which maintains that legal obligations apply regardless of the source or availability of personal data. Even though personal data scraping might be legal under the current Indian laws, according to section 8 (5) of DPDPA[29] a data fiduciary is required to protect personal data in its possession or under its control from personal data breaches. Therefore, to ensure compliance with the provisions of the Act, data fiduciaries should prevent the downloading of private media or impose limitations on how personal information can be shared on their platform. Moreover, according to Section 8 (6) of the Act[30], if a personal data breach occurs then the data fiduciaries are obligated to inform the Data Protection Board and the Data Principal about such a breach. Hence, it can be safe to say that even though technically India lacks a specific regulation regarding data scraping for training GenAI, there are sufficient remedies, both in existing as well as proposed legislations that can be availed, in case personal data is scraped without the express consent of the data principal.

Deepfakes and Data Protection under DPDPA 2023:[31] In India, the legal status of deepfakes is tricky to determine because creating a deepfake is not illegal per se unless it infringes upon the privacy of individuals, involves harassment, or engages in any activity forbidden by the law. Most Indian laws regarding data protection do not directly address the misuse of deepfake technology. This gap can leave the current legal framework ill-equipped to deal with privacy violations arising from the use of deepfake technologies.

[29] Digital Personal Data Protection Act 2023, s 8(5)
[30] Digital Personal Data Protection Act 2023, s 8(6)
[31] Digital Personal Data Protection Act 2023

Until specific legal guidelines are established for dealing with the problem of deepfakes, it is worth noting the existing legal provisions that could be utilized in dealing with the deepfake problem. Section 66D of the Information Technology Act, 2000[32] provides punishment for cheating by personation or impersonation fraud by using a computer resource. Therefore, a deepfake created to defraud an individual by impersonation could essentially be covered by this provision. Section 66E of the IT Act[33] becomes relevant in the context of pornographic videos created using deep learning algorithms. This section penalizes unauthorized publication or transmission of images of an individual's private area without consent, with imprisonment for three years and a fine of rupees 2 lakh. Furthermore, sections 67,[34] 67A[35], and 67B[36] of the IT Act prohibit and penalize the dissemination of obscene or sexually explicit material, including depictions involving children, in electronic form.

The DPDPA does not specifically deal with deep fakes, however, according to section 8(5)[37] of the Act, a data fiduciary is obligated to process personal data by taking reasonable security measures in order to prevent the personal data of the data principal from falling into the hands of malicious actors. Moreover, section 8(10)[38] provides for the establishment of an effective grievance redressal mechanism, which obligates the Data Fiduciary to adopt such measures necessary for preventing personal data breaches.

Rights of a Data Principal under the DPDPA:[39] Chapter III of the DPDPA sets out four essential rights of the data principal. Firstly, according to section 11 of the Act[40], a data principal shall have the right to access information about personal data in possession of the data fiduciary. Secondly, section 12[41] of the Act provides the right to review, correct, and erase personal data.

[32] Information Technology Act 2000, s 66(d)
[33] Information Technology Act 2000, s 66(e)
[34] Information Technology Act 2000, s 67
[35] Information Technology Act 2000, s 67(a)
[36] Information Technology Act 2000, s 67(b)
[37] Digital Personal Data Protection Act 2023, s 8(5)
[38] Digital Personal Data Protection Act 2023, s 8(10)
[39] Digital Personal Data Protection Act 2023
[40] Digital Personal Data Protection Act 2023, s 11
[41] Digital Personal Data Protection Act 2023, s 12

Thirdly, section 13[42] of the Act provides the right of grievance redressal and lastly, the Act provides for the right to nominate another person to exercise the rights of the data principal in the event of death or mental incapacity. Thus, Generative AI creators could be expected to satisfy requests for access, correction, and erasure which can be technically complex for such models. The black-box nature of many AI models can make accessing and modifying personal data embedded in the model parameters quite challenging as a data point invariably influences many parameters in complex ways during model training. Simply editing certain parameters by way of correction or removal may not achieve the desired results. Moreover, retraining large language models (LLMs) from scratch every time a data removal/modification request comes in would be extremely expensive and inefficient owing to the significant computational costs incurred during the training of LLMs. Overall, while these provisions under the DPDPA aim to uphold data principals' rights, implementing them effectively for complex machine learning systems remains an open technical challenge that will require further research breakthroughs.

CONCLUSION

The Digital Personal Data Protection Act (DPDPA) of 2023[43] represents a significant step towards establishing a comprehensive legal framework for data protection in India. However, the Act faces several challenges in addressing the unique complexities and evolving nature of AI systems. As India continues its journey towards becoming a global leader in AI, it must prioritize the protection of its citizens' privacy and personal data. By fostering a culture of transparency, accountability, and ethical AI development, India can harness the transformative potential of these technologies while upholding the fundamental rights and freedoms of its people.

In conclusion, the integration of AI into various sectors presents both opportunities and challenges. By addressing the legal and technical hurdles highlighted in this article, India can pave the way for a future where AI and data privacy coexist harmoniously, driving innovation while preserving the dignity and autonomy of individuals.

[42] Digital Personal Data Protection Act 2023, s 13
[43] Digital Personal Data Protection Act 2023