ISSN: 3048-9423(Online)
Naveen International Journal of Multidisciplinary Sciences (NIJMS)
© NIJMS | Vol. 2 | Issue 4 | February-March 2026
Available online at: https://nijms.com/
DOI: https://doi.org/10.71126/nijms.v2i4.117

EFFECT ON NEW TECHNOLOGIES ON THE RIGHT TO PRIVACY IN INDIA: WITH SPECIAL REFERENCE TO ARTIFICIAL INTELLIGENCE

Anand Kumar Sharma [1] & Prof. D. N. Diwedi [2]

[1]*Research Scholar, Department of Law, Meerut college Meerut UP.*
[2]*Professor, Department of Law, Meerut college Meerut UP.*
[1]***Corresponding Author Email:*** *anandsharmallb@gmail.com*

ABSTRACT:

The rampant development of new-age technologies like Artificial Intelligence (AI) has brought with itself several advantages, but it has also posed concerns to privacy rights. In Indian scenario, the privacy right has been affirmed as a constitutionally upheld guarantee, yet the legislative structure addressing AI and data protection seems to be nascent. AI applications mostly depend on the collection as well as processing of huge chunk of personal data, which could pertinently violate persons' privacy rights. Technologies such as deep learning algorithms and machine learning can expose insights and patterns from the database which might leak sensitive personal particulars. India lacks a robust data protection legal framework, despite the enactment of the "Personal Digital Personal Data Protection (DPDP) Act 2023". The enactment seeks to govern the processing of personal data & contains protective measures such as individual consent mandate and data localization. Still problems remain regarding potential exclusion of State agencies and whether the said Act sufficiently deals with the concerns specific to AI tools. The Indian Apex Court has clearly found that while privacy is a fundamental rights but it is not absolute. Striking balanced approach would be essential in this aspect for fostering responsible AI which seeks to improve the societal benefits without undermining the individual privacy. Comprehensive regulatory mechanism, ethical guidelines and governance frameworks are required for ensuring that AI development mirrors with the democratic ethos and constitutional sprits.

Keywords: *Privacy Rights, Artificial Intelligence, Data Protection, India.*

INTRODUCTION:

AI and the ever-evolving regulatory arena—both stress on the current situation of data protection and privacy issues. Preventing intrusion into another's life is the very essence of privacy. Almost each

individual now prioritize protection of their own sensitive data and privacy because of technological advancements. Preserving privacy becomes significant as individual's freedom might be curtailed when their data is obtained by ill-minded person. Privacy could be deemed as an approach to ensure data security. Every person are entitled to a "personal domain", free from arbitrary surveillance from state and third-party. The AI models depend on collection and processing of huge amount of personal information, which could potentially contravene the privacy right of a person. AI-based predictive policing technologies, facial recognition and surveillance techniques raises problems concerning mass profiling and monitoring. Although the government has enacted Digital Personal Data Protection Act 2023 for regulating the processing of personal data, it lacks in delving into the concerns associated with AI system. With AI emerging as a powerful new technology, it is significant to govern the AI as people rely heavily on such systems for accomplishing their task. Thus, the paper deals with the potential impact which is created by new-age frontier technologies like AI upon the essential right of privacy.

ARTIFICIAL INTELLIGENCE (AI) & ITS APPLICATIONS

The expression AI was propounded in the year 1956 by John McCarthy. He outlines that "AI is the science & engineering of developing intelligent machines". Peter Norvig and Stuart Russell provide the definition of AI as "the intelligent agents that utilize inputs called as precepts for observing their surrounding and then giving reaction by behaving in a manner that advances their objectives". Likewise, Patrick Milkalef and Manjul Gupta enunciate that "AI is the capability of the tool to recognize, interpret, make inference and thereby learning from the data for attaining predetermined societal and organizational objectives". Overall, it could be understood that AI imitates human intellect in computer devices which are having capability to carry out works that usually require human intelligence.

Some of the major applications of AI are:

(i) **Natural Language Processing (NLP):** It makes machines capable enough to understand and reproduce human language. Virtual assistants like Siri and Chatbots are suitable instance of its applications.

(ii) **Machine Learning:** Algorithms aided by AI enable applications to assess huge datasets and give predictions on the basis of insights and patterns. This is being used in marketing, medical, and financial sectors.

(iii) **Computer Vision:** AI-based systems can now easily interpret visual data from images and videos. It is applied in facial recognition tools, self-driving cards and surveillance technologies.

(iv) **Robotics:** AI-powered robotics encompasses the creation of applications which can autonomously conduct physical activities. Exploration, healthcare, and manufacturing all utilize robotics.

(v) **Personalization and Recommendation tools:** AI algorithms assess user conduct to offer appropriate content, service and product recommendations. Platforms such as social media, Amazon and Netflix feeds all make this evident.

RIGHT TO PRIVACY

Justice Nariman propounded the idea of privacy under the preamble of Indian Constitution by expressing that: *"The dignity of a person encapsulates the right of the person to develop ones capabilities, and this development can only take place when a person possess liberty and autonomy over fundamental control and decisions, on the sharing of personal information which can be contravened by unlawful use of this information".*

The Indian judiciary has liberally interpreted Article 21 of Indian Constitution for upholding privacy of an individual. However, this right is subject to reasonable restriction for preserving the security, integrity and sovereignty of the nation, morality, decency or public order and friendly ties with other nations.

The matter of ***"Justice K. Puttaswamy (A.D.) v. Union of India"*** is landmark victory for privacy rights. The petitioner questioned the constitutionality of Aadhar Card i.e., Indian biometric identity scheme. The 9-judges overwhelmingly confirmed that "the right to privacy is protected as an essential component of the right to life and personal liberty envisaged under Article 21 and as an element of freedoms enshrined under Part III of the Indian Constitution". However, the Supreme Court in the cases like *Mr X. v. Hospital, PUCL v. Union of India and Gobind v. State of Madhya Pradesh & Anr*. highlighted that persons are entitled to right to privacy under Article 21 of the Indian Constitution, but it is not absolute and subjected to exceptions like larger state interest.

Internationally, several international instruments recognize and uphold right to privacy. As per "Article 12 of the Universal Declaration of Human Rights (UDHR) 1948", the individuals are protected from arbitrary intervention into private space. Similarly, "Article 17 of the International Covenant on Civil and Political Rights (ICCPR)" reaffirms the significance of privacy right. The right to privacy has also been recognized under international conventions like "Article 8 of the European Convention on Human Rights and Article 16 of the Convention on the Rights of the Child, 1989".

NEXUS BETWEEN PRIVACY RIGHTS AND AI IN DIGITAL ARENA

The usage of AI systems is closely associated with the privacy rights. As cutting-edge technologies continue to grow at an unprecedented rate, the usage of AI has become a part of almost every field of our lives. AI has capabilities to transform the manner in which we engage with technology. With the expansion of presence in digital platform in routine life and the impact of virtual and physical worlds, a persons' private space expands far away from the physical private space. AI models don't only depend on massive amount of personal information of public for their growth, but they are also used in a manner which intrudes the private space. Because of this burning problem of privacy, it has become profound and pressing in current digital era. AI has become crucial medium to assist public manage their hectic lifestyle and complete works in faster and effective manner. But the major privacy issues concerning AI include the potential for unauthorized access and data breaches with respect to private data and thus there is an evident nexus between AI and privacy right.

HOW AI IS IMPACTING RIGHT TO PRIVACY

The potential to accomplish task more speedily than humans is one of the major factor why AI is becoming more attractive and demanding. With the assistance of AI tools, the massive volumes of database

can be easily analyzed and transmitted. AI through its machine learning skills has brought substantial improvement in computational algorithms by examining and optimizing the individual's voice recording, face picture, DNA and other crucial parameters. The wide accessibility of AI-based techniques has entered almost all facets of contemporary life. However in several cases, AI has compromised the individual's privacy. The prevalence of AI has evolved from self-driving vehicles to voice assistants to medical and diagnostic tests. Increasing concerns regarding AI are not merely its effect on corporate activities or its ethical effects but it is further about the privacy issue and cyber security threats.

(i) **Data Exploitation:** The data received through AI systems are sold to marketers and customers even don't know how much and in what manner their information are being processed, modified or divulged. AI can easily exploit these data in a fraction of a second. For instance, keyboard typing patterns of an individual could be utilized for deducing their mental and emotional state.

(ii) **Facial and Voice Recognition:** The utilization of voice and facial recognition technology (FRT) directly violates the free assembly and privacy. FRT is increasingly adopted by government to detect and watch their citizens, indirectly with a view to reduce crime, maintain national identity or more expressly to oversee dissidents. The private information is not kept confidential as law enforcement personnel might use them during their investigation with the use of AI applications. These systems are used to recognize, harass and detain peaceful protestors.

(iii) **Recognition and Tracking:** AI assists in identification and supervision of the persons, which again violate their privacy. AI applications could be adopted to recognize and detect persons by mapping their ongoing activities by examining private information from different gadgets such as smart watches and smart phone. AI differs between the non-personal and personal data through de-anonymization of anonymous information of the persons based on intervention caused from other gadgets. Today's AI models can generate 360-degree profile of person by obtaining information from different sources like social media application, card transactions and street cameras.

(iv) **Profiling:** It's quite common to abuse and exploit the personal data collected by AI profiling. The individual whose personal data is being obtained know nothing regarding the same and victim is helpless in such a scenario. Individual's sensitive data was hacked over various famous social media sites, including Amazon, Facebook. Apple and Google.

(v) **Prediction:** Predicting personal data from publicly accessible domain is the common use of ML and AI tools. The person's privacy is being undermined as their mood (joyful, confident, sad, etc), political opinion and sexual orientation could be accurately predicted. Such profiling could cause significant challenge to the privacy of an individual.

(vi) **Discrimination and Bias:** While developing AI applications, the developer shall incorporate data which lacks biasness and is non-discriminatory. The training of these systems shall be such that there is no scope for any form of biasness. An AI model utilized of recruitment might perpetuate discrimination against certain community when the data was trained on discriminatory data.

(vii) **Mass Surveillance:** AI-driven surveillance tool has potential to continuously monitor large population which promotes intrusive and pervasive supervision of persons' daily activities, which

hinder privacy rights. Thus, another potent issue is the adoption of AI for surveillance. Facial recognition techniques, aided by AI, are being used by individuals, corporations and State for tracking and monitoring people. This poses a significant issue regarding privacy rights. Although these advancements could be utilized for security reasons like curbing terrorism or recognizing offenders, they also widen the scope for unlawful surveillance by corporations or State. For instance, the facial recognition technology used by Clearview AI gathers all the publicly accessible pictures from the online platform for creating a huge database, thereby raising grave privacy issue and concerns of massive surveillance in several ways.

EXISTING LEGAL FRAMEWORK GOVERNING PRIVACY LAW IN INDIA AND SHORTFALLS IN THE AI ERA

Indian government has adopted profound efforts in identifying and governing data privacy in past few years. A notable progress came with the framing of the Digital Personal Data Protection (DPDP) Act 2023, which seeks to formulate norms for addressing digital personal data and assure that person's data is processed in lawful manner. The enactment is premised on the principle of data minimization, object limitation, and consent. It also incorporates the concepts such as "data principals" and "data fiduciaries" for defining the rights of individuals and the obligations of data collectors. The Act enunciates that data fiduciaries are bound to obtain express consent from user for data handling and withdrawal. Data Principal possesses right to access, edit or even delete their personal information. Non-adherence could lead to fine up to 30 million dollars (around 250 crore Rupees). But the DPDP Act has lacunae concerning AI. The enactment excludes governmental institutions, raising issues regarding smart city surveillance and Aadhar.

Another significant legislation is the "Information Technology Act 2000", which regulates data security and electronic communication. The Act contains section relating to cyber-crime and safeguarding of sensitive personal information under its rules like "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011". Section 43A of the Act prescribes for compensation in case of violation of data privacy caused because of negligent treatment of private data. This Section could be used in the scenario of AI models which handle user information. Further, Rule 4(4) of the IT Rules 2021 obligates that "significant social media intermediaries" shall ensure that AI-based application doesn't cause hindrance against user rights, particularly with respect to misinformation and content moderation. But these statutes mainly stress on online content and data collection, fails to directly deal with the complexities introduced by AI tools such as eliminating bias and imposing algorithmic accountability.

Critical Gaps

(i) **Absence of AI-dedicated Law & potential concerns:** Although legal framework addressing data privacy in India provides guidelines for protection of personal information, they didn't account for the specific requirements of AI models. AI system mostly needs continuous access to huge database for improving their algorithm, which can eventually result into unintended consequences when persons' data is processed in a manner they didn't expressly consent to. As AI models develop,

ensuring that the sensitive information used to train these systems is properly protection becomes important challenge.

(ii) **Algorithmic Accountability and Transparency:** AI technologies are usually opaque, making it problematic for persons to comprehend how decisions are being adopted on the basis of data. Such lack of transparency give rise to significant issue, especially in the field of law enforcement, credit scoring, and hiring decisions. The lack of accountability measures for users and developers of AI tools further perpetuate the problem. The present data privacy law like DPDP Act and PDP Bill, lack provisions which particularly govern the transparency of AI-based decision-making.

(iii) **Cross-border Data Transfer and Data Sovereignty**: India's growing dependence on international AI forums raises issues regarding the sovereignty of its citizens' information. With several AI applications relying on outsourcing data processing and cloud services, private information is mostly stored and processed beyond Indian Territory. Although the DPDP Act seeks to regulate cross-border flows, it doesn't fully address the issues created by the transnational nature of AI models, which might function across the borders in a manner which dilutes the Indian data protection legislations.

COMPARATIVE EXAMINATION WITH SELECTED JURISDICTIONS

Various foreign jurisdictions have attempted to handle privacy rights in AI, which has been dealt below:

United States: US don't have AI-specific legislation but it addresses AI-based activities through agencies. The Federal Trade Commission functions to ensure AI transparency by mandating evident and comprehendible disclosures regarding how AI system work and to avoid all the biased decision-making by making corporations absolutely liable for discriminatory practices. Likewise, US federal agency, "National Institute of Standards and Technology" lays down AI threat management structure. Further, the White House AI Bill of Right aims to empower persons to have control over their private information and safeguards all citizens from harmful AI practice.

China: The Chinese AI legislative structure primarily stress on the AI ethics, data control and national security. The AI developers are bound to comply with interim measures for management of Generative AI Services. The rule deals with several of problems concerning utilization of generative AI like personal data protection, content security, data security, and intellectual property infringement.

Europe: The EU's Artificial Intelligence Act contains robust framework for AI models across the Europe. The legislation divides AI applications into 3 risk-based categories: unacceptable risk, high risk and low risk. Models with unacceptable risk are deemed dangerous and are majorly forbidden. This entails systems which indulge into social scoring, facial recognition, biometric identification and behavioral manipulation.

SUGGESTIONS FOR STRENGTHENING THE DATA PRIVACY LAW IN AI

(i) Introduction of AI-Specific Privacy Law: For addressing the problems created by AI and taking lessons from the comparative illustration, Indian government shall enact legislations that especially cater to the complexities of AI technologies within private space of an individual.

(ii) Ensuring Privacy-by-Design: AI models shall introduce privacy-by-design norms, ensuring that users have more control over their information, sensitive information is encrypted and data processing

is minimized. These measures will assist in mitigating threat by integration of privacy concerns into the development mechanism.

(iii) **Impose Algorithmic Accountability and Transparency:** AI models should evidently describe how they utilized the personal information to arrive at a decision. Transparency models should be incorporated which ensures trust and enable effective redresses. A national framework shall be established for independent audit of AI models with a view to examine the bias, transparency and adherence with legal and ethical rules.

(iv) **Strengthening Enforcement**: For ensuring compliance of data privacy over AI realm, India shall constitute a specific data protection authority casted with the responsibilities to supervise the use of AI models and their effect on privacy of an individual. This authority shall be authorized to audit AI systems, levy penalties for privacy violations and assure that companies give effect to the law.

(v) **Raising Public Awareness:** The State should launch public awareness workshops and campaigns for sensitizing persons regarding their rights under data protection framework and how they could safeguard their private data.

CONCLUSION

The introduction of AI has found out to be a great potential, but it still creates substantial hindrance to the preservation of right to privacy. Given the nation's speedy digitalization & increasing adoption of AI in several sectors, State shall undertake appropriate efforts for addressing potential privacy issues. It would be a significant aspect to strike optimal balance between promoting innovation and protection fundamental rights like privacy. For ensuring responsible AI development which fosters socio-economic benefits without comprising individual privacy, it is crucial to have comprehensive regulatory sandboxes, ethical norms and governance structures. For upholding privacy in a world which is highly influenced by AI, it is essential to inculcate a collaborative strategy that engages relevant stakeholders like the state, civil society, industry and public at large.

REFERENCES

[1] Ashish Kumar Singh, 'Convergence of Artificial Intelligence and Privacy Rights in India's Legal Framework' (2025) 7(4) *International Journal for Multidisciplinary Research* (IJFMR) https://www.ijfmr.com accessed 16 December 2025.

[2] Chinmayi Arun, 'Privacy and the Constitution of India' (2019) 14 *NUJS Law Review* 1.

[3] Constitution of India 1950, art 21.

[4] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, adopted 4 November 1950, entered into force 3 September 1953) art 8.

[5] Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 art 16

[6] D. Majumdar and H.K. Chattopadhyay, "Emergence of AI and its implication towards data privacy: From Indian legal perspective," IJLMH, Volume 3 | Issue 4 (2020).

[7] Digital Personal Data Protection Act 2023 (Act No 22 of 2023, India).

[8] European Union Agency for Fundamental Rights, *Getting the Future Right: Artificial Intelligence and Fundamental Rights* (Publications Office of the EU 2020).

[9] Frank Pasquale, *New Laws of Robotics* (Harvard University Press 2020).

[10] Information Technology Act 2000 (India).

[11] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India)

[12] Information Technology Act 2000 (India), s 43A.

[13] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India), r 4(4)

[14] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 art 17.

[15] J. Nissha, "Critical Analysis of Right to Privacy in India," International Journal of Law Management & Humanities, Volume 6 | Issue 1 (2024).

[16] Justice BN Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Government of India 2018).

[17] K.S. Puttaswamy v. Union of India

[18] Margaret A Boden, *Artificial Intelligence: A Very Short Introduction* (OUP 2018).

[19] Mimi Zou and Lu Zhang," Navigating China's regulatory approach to generative artificial International Peace, 2024 intelligence and large language models", Cambridge University Press, 06 January 2025, available at https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governance/article/navigating-chinasregulatory-approach-to-generative-artificial-intelligence-andlarge-languagemodels/969B2055997BF42DE693B7A1A1B4E8BA

[20] Nick Lawrence, AI in UI, 2323 and Beyond, Medium(28th August, 2024) https://uxplanet.org/ai-in-ui-2023-and-beyond-346b4602eff7

[21] Nils J Nilsson, *The Quest for Artificial Intelligence* (Cambridge University Press 2010).

[22] Patrick Mikalef and Manjul Gupta," Artificial intelligence capability: Conceptualization, measurement calibration, and empirica.

[23] *People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301.

[24] Prof Dalvinder Singh Grewal, "A Critical Conceptual Analysis of Definitions of Artificial Intelligence as Applicable to Computer Engineering",16 IOSR Journal of Computer Engineering 10 (2014)

[25] Ryan Calo, 'Artificial Intelligence Policy: A Primer and Roadmap' (2017) 51 *UC Davis Law Review* 399.

[26] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR' (2017) 7 *International Data Privacy Law* 76.

[27] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2021).

[28] Stuart Russell and Peter Norvig," Artificial Intelligence A Modern Approach", Pearson Series In Artificial Intelligence 54,2022

[29] S.B. Rohith and N. Sethupriya, 'A Study on Impact of Artificial Intelligence on Right to Privacy in India' (2024) 4(3) *Indian Journal of Legal Review* (IJLR) https://iledu.in accessed 16 December 2025.

[30] The Impact of AI on Right to Privacy in the Digital Age' *Lawful Legal* https://lawfullegal.in/the-impact-of-ai-on-right-to-privacy-in-the-digital-age/ accessed 16 December 2025.

[31] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217A (III)) art 12.

[32] Usha Ramanathan, 'Aadhaar: From Welfare to Surveillance State' (2014) 49 *Economic and Political Weekly* 38.

[33] Woodrow Barfield and Ugo Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar 2018)

Cite this Article:

Anand Kumar Sharma and Prof. D. N. Diwedi*," *EFFECT ON NEW TECHNOLOGIES ON THE RIGHT TO PRIVACY IN INDIA: WITH SPECIAL REFERENCE TO ARTIFICIAL INTELLIGENCE*", *Naveen International Journal of Multidisciplinary Sciences (NIJMS), ISSN: 3048-9423 (Online), Volume 2, Issue 4, pp. 01-09, February-March 2026. Journal URL: https://nijms.com/

DOI: *https://doi.org/10.71126/nijms.v2i4.117*