International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ARTIFICIAL INTELLIGENCE AND PRIVACY CONCERNS

Dr Amrita Rathi[1*], Ms Upagya Sharma[2]

[1*]Associate Professor, University Institute of Legal Studies, Chandigarh University, Mohali 140413, Punjab, India
[2]Assistant Professor, Army Institute of Law, Mohali 160062, Punjab, India

1. Abstract

From virtual assistants like 'Siri' and 'Alexa', to autonomous vehicles and facial recognition systems – the AI technology is permeating our daily lives and raising privacy concerns especially regarding personal data. AI systems often rely on vast data to train their algorithms and improve performance. This data can include personal information such as names, addresses, financial information, and sensitive information such as medical records. The collection and processing of this data can raise concerns about how it is being used and who has access to it. With so much data being collected and processed, there is a risk that it could fall into the wrong hands, either through hacking or other security breaches.

Generative AI can be misused to create fake profiles or manipulate images or create 'deepfakes'. Like all other AI technologies, it also relies on data. Cybercrimes affect the security of 80% of businesses across the world. Another concern is the use of AI for surveillance and monitoring purposes. Facial recognition technology, for example, has been used by law enforcement agencies to identify suspects and track individuals in public spaces. This raises questions about the right to privacy and the potential to abuse these technologies.

AI technologies are becoming more advanced, allowing them to collect and analyse significant amounts of data about individuals, including their behaviours, preferences, and even their thoughts and emotions. This information can be used to make predictions about individuals, to target them with advertising or other marketing messages, or even to make decisions about their access to services or opportunities.

2. Meaning and Concept of Privacy and Artificial Intelligence

The word 'privacy' has been derived from the Latin word '*privatus*' which means *'set apart*'. Privacy is the ability of an individual or group to seclude them or information about themselves and to reveal them selectively. It is "the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and circumstances to communicate with others. It means his right to withdraw or to participate as he sees fit, the individual's right to control dissemination of information about him; it is his own personal possession".

Privacy is often associated with anonymity, the wish to remain unnoticed or unidentified in the public realm. The degree to which any private information is exposed depends on how the public will receive this information, this varies between places and over time. Privacy can be perceived as an aspect of security in which trade-offs between the interests of one group and another can become particularly clear. Numerous legal and moral philosophers have suggested that privacy is valued because it satisfies a number of primary human needs. There are various dimensions of privacy including physical privacy, psychological privacy, social privacy, and informational privacy. They are correlated. Physical privacy refers to individual's right not to be supervised (in his private space). Social privacy applies to individual's right to avoid unwanted communication and to have the right to intimacy and security. Psychological privacy refers to individual's right to be able to express his opinion, feelings and beliefs without any pressure and interference.

In the age of internet, invasion of informational privacy is a significant issue which increases with the user's inability to control the collection, storage, and usage of information about their online

Received: August 13 , 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

activity. Both users and the media are focused on issues such as various types of personal information misuse, ranging from spam and online marketing activities to more dangerous ones, like identity or credit card theft. The concept of online privacy is influenced by the perception of the degree of supervision, intimacy, security and freedom to express one's opinion in an online environment without the apprehension of negative consequences. Only a limited number of researchers have investigated various factors of users' online privacy perception. Mary Madden, worked on understanding the public perceptions after the Snowden revelation, relating to the government accumulating data to about the individuals.

According to Britannica Dictionary: Artificial intelligence (AI), the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience. Since their development in the 1940s, digital computers have been programmed to carry out very complex tasks—such as discovering proofs for mathematical theorems or playing chess—with great proficiency. Despite continuing advances in computer processing speed and memory capacity, there are as yet no programs that can match full human flexibility over wider domains or in tasks requiring much everyday knowledge. On the other hand, some programs have attained the performance levels of human experts and professionals in executing certain specific tasks, so that artificial intelligence in this limited sense is found in applications as diverse as medical diagnosis, computer search engines, voice or handwriting recognition, and chatbots.

3. Artificial Intelligence Systems and Data Dependence

Data as the Foundation of AI: Most contemporary AI models, particularly machine learning and deep learning systems, require vast amounts of data to identify patterns and make predictions. This includes:

- Personal identifiers (names, addresses, phone numbers)
- Behavioral data (browsing history, purchasing habits)
- Biometric data (faces, fingerprints, voice patterns)
- Health and financial records

As AI systems grow more complex, so do the privacy risks associated with their data inputs and outputs.

Inference Risks: Even when raw data is anonymized, AI models can make sensitive inferences about individuals. Examples include predicting mental health status, political affiliation, or socioeconomic background. Such inferences raise ethical and legal challenges, as individuals may be unaware that these predictions are being generated or used.

4. Privacy Challenges in Artificial Intelligence

- **Surveillance and Loss of Anonymity:** AI-powered surveillance systems, including facial recognition and behavioral analytics, can track individuals in public and private spaces. This undermines anonymity—a foundational aspect of privacy and enables mass surveillance, which may be exploited by governments, corporations, or malicious actors.
- **Data Breaches and Security Risks:** AI systems often store large quantities of sensitive information, making them attractive targets for cyberattacks. A breach can expose personal data of millions, leading to identity theft, reputational harm, and other long-term consequences. Furthermore, AI models themselves may leak training data (a phenomenon known as *model inversion*).
- **Algorithmic Bias and Discrimination:** Although technically distinct from privacy, algorithmic bias intersects with privacy concerns because biased datasets can amplify inequalities. When AI predicts attributes about individuals, these predictions can be unfair or discriminatory, affecting access to jobs, credit, healthcare, or government services.

Received: August 13 , 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- **Lack of Transparency and Explainability:** Many AI systems function as "black boxes," providing results without clear explanations. This obscurity makes it difficult for individuals to understand how their data is used or challenge decisions made by AI.

5. Regulatory and Ethical Considerations

Global Privacy Regulations: Several jurisdictions have introduced regulations governing data collection, AI deployment, and privacy protection:

- **GDPR (European Union):** Provides strict guidelines for data protection, algorithmic transparency, and user consent.
- **CCPA/CPRA (California):** Grants consumers rights over personal data collected by companies.
- **AI Act (EU)**: Aims to regulate AI systems based on risk categories.

Despite progress, global regulatory approaches remain inconsistent, creating challenges for cross-border AI deployment.

Ethical Frameworks: Non-legislative frameworks also guide AI development:

- The OECD AI Principles
- IEEE Ethically Aligned Design
- UNESCO AI Ethics Framework

These emphasize principles such as transparency, accountability, fairness, and respect for human rights.

Technological Solutions to AI Privacy Risks

- **Differential Privacy:** This technique introduces statistical noise into datasets, preventing identification of individuals while preserving overall data patterns.
- **Federated Learning:** Data remains on local devices, and only model updates are shared for aggregation. This reduces the risk of centralized data breaches.
- **Homomorphic Encryption:** This enables computation on encrypted data, ensuring that sensitive data remains unreadable throughout processing.
- **Data Minimization and Synthetic Data:** Instead of collecting raw user data, systems can use synthetic or minimized datasets to reduce privacy exposure.

6. Legislative Framework in India

- An Overview- India has historically relied on piecemeal provisions under the Information Technology Act, 2000 and related rules for data protection. The landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC recognised the *right to privacy* as a fundamental right under Article 21 of the Constitution.
- In August 2023, the DPDP Act, 2023 was enacted to establish comprehensive safeguards. It applies to the processing of digital personal data, imposes duties on data fiduciaries, and recognises rights of data principals, including the right to access, correction, and grievance redressal. However, the Act is largely technology-neutral and does not contain AI-specific provisions.
- AI's integration into daily life has caused a revolution in industries while also bringing up big legal issues about data privacy. India's Digital Personal Data Protection (DPDP) Act, 2023 has created a legal system to protect personal data. But the quick progress in AI tech makes it hard to enforce and use this law well. This article looks at how AI and data privacy overlap examining the conflicts between AI's need for data and the DPDP Act's aim to protect. It breaks down legal terms, looks at real cases, and considers practical effects to untangle the complex issues and suggest how to balance new ideas with people's rights.
- AI and data privacy clash creating a tricky balance between new tech and people's safety. AI needs lots of private data, which goes against key privacy ideas like getting permission to use less

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

data and using it for specific reasons. The main problems come from people losing control over their information. AI systems often use data without asking or explaining, which can lead to misuse of personal details. This affects people's lives in big ways. For example, AI in banks might deny loans to certain groups. Also, face-scanning cameras can invade privacy. This creates a world where people don't know how companies collect, study, and use their data making them feel helpless and distrustful of tech. The Digital Personal Data Protection Act 2023, tries to fix these issues. But it's hard to balance AI's potential with people's basic rights, as AI needs lots of data, which often goes against legal protections.

- The DPDP Act, 2023 brings to the front several provisions that in the first place are put in place to protect personal data. Section 4 stresses the importance of permission, while Section 6 reiterates the necessity of data minimization. These principles are parallel with the global data protection guidelines, for instance, the GDPR. Besides that, AI systems, especially the ones that operate with machine learning, enjoy having access to diverse and large datasets—often a result of collecting data without explicit, informed consent. Hence, this paradox is the catalyst, which suggests that the DPDP Act might cursorily stunt AI formation.
- Consent and Transparency: The Act obliges concise and categorical consent to data processing. However, AI algorithms often do not have explainability, compromising the effort of informing users accurately how the data will be used.
- Purpose Limitation: AI models may be developed to bring about flexibility but in the process, they might start using data for other purposes. This contradicts the Act, which requires data processing to be kept within the set objectives.
- Cross-Border Data Transfer: The global nature of AI platforms necessitates data sharing across jurisdictions. The DPDP Act's stringent regulations on cross-border data transfer add another layer of complexity.

8. Conclusion

Artificial Intelligence offers transformative benefits, but these advancements come with significant privacy challenges. From mass surveillance to data exploitation, AI systems can threaten fundamental rights if left unchecked. However, through robust regulations, ethical design principles, and technical innovations, society can harness AI's potential while preserving privacy. The future of AI depends on building systems that respect human autonomy, ensure fairness, and safeguard personal data. Responsible governance and continued research are vital to maintaining this balance as AI becomes further integrated into daily life.

References

1. Brundage, M., et al. (2020). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.*
2. Floridi, L. (2019). *Establishing the rules for building trustworthy AI.*
3. Goodman, B., & Flaxman, S. (2017). *European Union regulations on algorithmic decision-making and a "right to explanation."*
4. O'Neil, C. (2016). *Weapons of Math Destruction.*
5. Solove, D. J. (2021). *Understanding Privacy.*
6. https://www.brookings.edu/articles/protecting-privacy-in-an-ai-driven-world/
7. Mary Madden, "Public Perceptions of Privacy and Security in the Post-Snowden Era", November 12, 2014, Pew Research Centre
8. <https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/
9. https://www.etymonline.com/word/privacy
10. Madhavi Divan, "The Right to Privacy in the Age of Information and Communications", 4 *SCC (Jour)*, 12 (2002)

Received: August 13 , 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

11. Sioerd Keulen and Ronald Kroeze, "Privacy from a Historical Perspective", *Amsterdam University Press*, 21-56 (2018).
12. https://lawfullegal.in/the-intersection-of-ai-and-data-privacy-challenges-under-indias-digital-personal-data-protection-act-2023/

Received: August 13 , 2025