RIGHT TO PRIVACY AND ARTIFICIAL INTELLIGENCE: A CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Neha Bhuwania, LLM-SOL Presidency University

Kishore Kumar D, LLM-SOL Presidency University

ABSTRACT

Artificial Intelligence (AI) is increasingly becoming an integral part of our lives, impacting decision-making in sectors such as health, finance, governance and digital services. AI offers efficiency, innovation and convenience, but it also presents significant privacy challenges.

AI's reliance on vast, often sensitive, personal data sets and opaque decision-making processes fundamentally disrupts conventional notions of consent, data security, and individual autonomy. In the Indian context, the enactment of the Digital Personal Data Protection (DPDP)Act, 2023 marks a foundational step in regulating personal data processing. Yet, while the Act incorporates key principles such as shared consent, data minimization, and lawful processing, it remains insufficient to address the distinct and evolving privacy risks introduced by AI technologies. Issues such as algorithmic bias, re-identification of anonymized data, AIdriven surveillance, and obscurity in automated decisions continue to challenge the existing regulatory framework.

This article critically examines these emerging issues, highlighting the gaps in India's legal infrastructure and comparing them with global regulatory practices like the 'European Union's General Data Protection Regulation' (GDPR) and the EU AI Act. It advocates for a multi- layered strategy to strengthen Privacy protection in the AI era, including embedding privacy by design, enhancing algorithmic transparency, adopting AI-specific legal reforms, and promoting digital literacy among users.

The paper concludes by emphasising the importance on unified action by governments, industry, civil society, and individuals to develop AI systems that are ethical, accountable, and privacy-respecting. Only through continuous, adaptive, and inclusive policy-making can India and the global community strike a sustainable balance between harnessing AI's transformative potential and safeguarding individual privacy rights in an increasingly data-driven world.

Keywords: DPDP Act, Data Privacy, Implementation Challenges, Artificial Intelligence, Right to Privacy, Fundamental Right, Constitution of India

1. INTRODUCTION

We are in the 21st century of data. We generate a lot of personal data every day, from social media to financial and medical data. This data is crucial for a powerful technology called Artificial Intelligence (AI). It enables machines to learn, predict and make decisions, sometimes independently.

AI has made our lives better, but it has also changed privacy. Privacy, once a matter of physical space and secrecy, now involves digital footprints, behavioural patterns and predictive profiling. We are not just users, but also data suppliers.

In India, the recognition of privacy as a fundamental right was a turning point when the Supreme Court declared Right to privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India [1], thereby signalling the need for a comprehensive data privacy law in India. Prior to the DPDP Act, the Information Technology Act, 2000 was the main law that protected the right to data privacy, but it was not adequate to address contemporary data privacy issues.

The Digital Personal Data Protection Act, 2023[2] was introduced to regulate the processing of personal data, based on this right. The DPDP Act aims to do this by establishing a consentbased data protection framework and clarifying the rights and responsibilities of data principals and data fiduciaries.

But data protection is not achieved by regulation alone[3]. The effectiveness of the DPDP Act[4] is heavily reliant on the approach and institutional framework. The adequacy of DPDP Act for data protection is examined in the context of implementation challenges.

In the light of the fast evolving AI, it is important to evaluate this legislation. This article explores the relationship between AI and privacy, the DPDP Act and the need for stronger

[1] Justice K.S. Puttaswamy (Retd*.) v.* Union of India*,* (2017) 10 SCC 1.
[2] Digital Personal Data Protection Act, 2023,S 4–11, 17–20.
[3] Ministry of Electronics and Information Technology, Digital India Programme, Government of India, available at: https://www.digitalindia.gov.in
[4] Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code [hereinafter "DPDP Act"]; Information Technology Act, 2000, No. 21 of 2000, India Code [hereinafter "IT Act"].

protections.

This article seeks to answer this question by considering the DPDP Act in relation to emerging AI challenges.

2. THE RIGHT TO PRIVACY: EVOLUTION AND IMPORTANCE

2.1 Privacy in India

Privacy was not mentioned in the Constitution. Its existence was long debated. However, privacy was eventually recognised by the courts, where the courts began to recognise privacy as a facet of the Right to Life and Personal Liberty under Article 21.

In the initial cases of M.P. Sharma[5] and Kharak Singh[6], privacy was narrowly construed, but in subsequent cases like Gobind and PUCL, it was construed more broadly. The turning point came in 2017, when the Supreme Court in the landmark case of Justice K.S. Puttaswamy v. Union of India established privacy as a fundamental right, linked to Articles 14, 19 and 21. This not only corrected earlier narrow readings but also laid the foundation for modern data protection.

In response, India passed the Digital Personal Data Protection Act (DPDP Act), which emphasises consent, data minimisation and corporate responsibility. But while the Act aligns India with global standards, it does not address concerns specific to AI, and the privacy versus national security, surveillance and corporate misuse of data[7].

2.2 International Recognition of Privacy

Privacy has been acknowledged internationally in human rights law. The Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) protect against arbitrary interference[8]. Europe went further with the European Convention on Human Rights, and then the General Data Protection Regulation (GDPR) in

[5] M.P. Sharma v. Satish Chandra, 1954 SCR 1077
[6] Kharak Singh v. State of U.P., AIR 1963 SC 1295
[7] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).
[8] Universal Declaration of Human Rights, 1948, Art. 12

2018 [9].

GDPR set standards for data collection and processing, the "right to be forgotten" and was influential. Its "Brussels Effect"[10] resulted in laws in Brazil (LGPD)[11], China (PIPL)[12] and U.S. states (CCPA/CPRA)[13]. But there are still challenges for the world: data transfers, government surveillance, data-hungry tech giants, and new privacy concerns with new technologies like AI[14].

So, in summary, India and the world have made great strides in recognising privacy as a human right. But with the rapid development of technology, we need to update our laws and work together to protect privacy in our increasingly connected world.

2.3 Importance of Privacy

Privacy is not just about secrecy, it is about control of personal information. It enables us to make choices, to exercise our autonomy and to preserve our dignity and freedom. In the case of informational privacy, the digital era has become increasingly important, especially with the advent of the artificial intelligence, which is increasingly dependent on the collection, processing and analysis of personal information

2.4 The Rise of AI

Artificial Intelligence (AI) refers to machines and systems that can perform tasks that typically require human intelligence, such as learning, reasoning and decision-making [15]. AI is now an important part of many industries, such as health care, where it is used for diagnosis and treatment; banking, where AI is used to prevent and detect fraud; e-commerce, where AI is used to make recommendations; and in government, especially in the creation of smart cities and surveillance. Although AI has a tremendous positive impact on efficiency and convenience, it leads to an increased dependence on large volumes of personal data, which establishes a

[9] European Convention on Human Rights, 1950, Art. 8
[10] Apar Gupta, The Battle for Digital Privacy in India (2022)
[11] Aziz Z. Huq, "A Right to a Human Decision", 106 Virginia Law Review 611 (2020).
[12] Nizan Geslevich Packin & Yafit Lev-Aretz, "Learning Algorithms and Discrimination", 94 Washington Law Review 459 (2019)
[13] Ari Ezra Waldman, Privacy as Trust: Information Privacy for an Information Age (2018).
[14] Lei Geral de Proteção de Dados, 2018 (Brazil).
[15] Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach, 4th edn. Pearson (2021).

critical and direct relationship between the development of AI and the new privacy challenge

2.5 Privacy Issues in the Age of AI

The growing integration of artificial intelligence in our lives has brought about a number of privacy and security issues. One of the main issues is the gathering of large volumes of data with inadequate consent. AI systems continuously gather data from social media, biometric information, wearables, online payments and smart devices, often without users' explicit consent.[16] Even when consent is obtained, it is often presented in long, complex documents or "click-to-agree" statements, which are hard to understand. Moreover, data is often used for new purposes without fresh consent (known as "purpose creep"), breaching the right to informational self-determination. Another issue is algorithmic bias and transparency. AI systems learn from historical data, which can reinforce and entrench biases, leading to discrimination in hiring, credit scoring and law enforcement. The "black box" nature of many AI systems also plays a role, as people may not understand or challenge decisions made about them. Responsibility is also diffuse, with multiple parties involved (such as developers, deployers and data providers), creating legal loopholes.

AI-based surveillance and profiling also present risks, as facial recognition, predictive policing and location tracking technologies enable mass surveillance[17]. These technologies can infer sensitive information, such as political beliefs or mental health, from seemingly benign data, compromising anonymity and potentially restricting freedom of movement and speech. This profiling and discrimination disproportionately impacts marginalised communities. Data security vulnerabilities also pose a risk.[18] AI relies on large, centralised data sets, which are attractive targets for cyber-attacks. Emerging threats such as model inversion, membership inference and data poisoning present risks that may not be fully addressed by current security protocols, and require AI-specific security protocols.

Further, the large data sets increase the risk of data theft and breaches. Finally, there are regulatory challenges. While India's DPDP Act provides a basic framework for data protection, it does not cover AI-specific issues, such as algorithmic audits, explain ability and the right to contest automated decisions. The broad exemptions for government agencies also pose

[16] High-Level Committee on Non-Personal Data Governance (Kris Gopalakrishnan Committee Report, 2020).
[17] Sandra Wachter et al., "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR", (2017) 7 International Data Privacy Law 76
[18] Centre for Democracy & Technology (CDT), AI Governance and Privacy (2023)

surveillance concerns. Globally, the lack of a consistent regulatory approach leads to confusion and difficulties in enforcement and accountability, highlighting the need for more comprehensive governance approaches[19].

3: DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a landmark legislation in India. This is the first time that India has a specific legislation regulating the collection, processing and protection of digital personal data. In an era where data knows no borders and no technology, this law seeks to encourage innovation while safeguarding rights, so that privacy is not sacrificed in the name of technological progress [20].

3.1 Scope and Applicability

The Digital Personal Data Protection (DPDP) Act is intentionally limited to digital personal data, i.e. any data relating to an identifiable individual, which is in digital form. The Act is wide in scope in that it is not only confined to data that is processed in India, regardless of where the data principal is located, but also to data that is processed outside of India, provided the processing is in connection with goods or services offered in India. However, the Act also explicitly excludes non-digital data, i.e. paper-based data, from its scope, thereby restricting its application to the digital world, where the potential for misuse is the highest. This extraterritoriality implies that India understands that data is global in nature and that data protection should not be constrained by territorial considerations.

3.2 Key Concepts

The Act defines two key concepts that are integral to its functioning, the Data Principal and Data Fiduciary. The Data Principal is the person to whom the personal data belongs, that is, anyone whose data is being obtained, stored or processed online. The Data Fiduciary is the entity, usually a business, government or organisation that decides the purpose and means of acquiring such personal data. It implies a trust relationship, which means that the entity must process data fairly and transparently. This conceptualisation will be consistent with international data protection laws, but will be expressed in terms that are specific to the Indian

[19] Reza Shokri et al., "Membership Inference Attacks Against Machine Learning Models", Proceedings of the IEEE Symposium on Security and Privacy (2017)
[20] Digital Personal Data Protection Act, 2023, No. 22 of 2023, S 4–11, 17–20 (India)

legal framework [21].

3.3 Rights of Individuals

The DPDP Act is largely concerned with empowerment of individuals as it provides a set of rights to regain control over personal data. They have the right to data, which means that they can know what data is being collected and for what purpose. They also have the right to rectification and erasure, which means that they can correct the inaccuracies and request the removal of irrelevant or outdated data. The Act also includes the right to redressal of grievances, which means that grievances can be redressed in a timely fashion. Crucially, individuals have the right to withdraw consent, it is not irreversible and can be withdrawn at any time. All of these rights would empower individuals and take the power away from corporations and institutions, and strengthen the idea of privacy as a right[22].

3.4 Responsibilities of Data Fiduciaries

Rights come with responsibilities and the DPDP Act imposes very high standards on data fiduciaries to be responsible for personal data. It mandates that the data should only be collected with the consent of the individual, which is explicit and informed, and therefore stresses transparency and choice. Further, data fiduciaries must also ensure the security of personal data by adopting appropriate security safeguards to prevent breaches, leaks or misuse. The principle of data minimisation is also emphasised and it requires that only the data necessary for the purpose should be collected-no more and no less.

3.5 Data Protection Board

The Act establishes the Data Protection Board of India as an enforcement authority. The Board can investigate data breaches, impose penalties on non-compliant or errant data fiduciaries, and safeguard individual rights by ensuring that any breaches are addressed in a timely and responsible manner. In doing so, it plays a crucial role in safeguarding individual rights, giving life to the Act. The establishment of the Board is a reflection of India's commitment to institutionalise data protection, moving from the world of policy to the world of practice.

[21] Solon Barocas & Andrew D. Selbst, "Big Data's Disparate Impact", (2016) 104 California Law Review 671
[22] Lilian Edwards & Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For", (2017) Duke Law & Technology Review.

4: ASSESSING THE DPDP ACT IN THE AGE OF AI

Artificial Intelligence (AI) is data-driven. Machine learning algorithms learn and make decisions based on large volumes of personal data. In this regard, the Digital Personal Data Protection Act, 2023 (DPDP Act)[23] is a welcome move for privacy in India. But from an AI point of view, the Act has some positives and negatives.

4.1 Strengths of the Act

The DPDP Act has some key strengths that make it more effective in safeguarding personal data in the digital era. Perhaps the most notable strength is that it is privacy-centred and helps to ensure a consent-based approach, where data processing is based on informed and revocable consent. This is especially important in an AI society where people have no choice in how their data is used, and the law helps to reclaim control over their digital identity. The Act also emphasises the responsibility of data fiduciaries by holding the parties that process personal data accountable, which helps to avoid their avoidance of responsibility due to the technological nature of the data processing, particularly in the case of AI systems that can be biased. The new severe penalty regime, including fines of up to ₹500 crore, also helps to ensure compliance and acts as a deterrent to misuse of the data, as the trust breach is a serious issue with far-reaching implications.

Further, the Act will bring the Indian data protection law in line with the global standards like the GDPR, which will help in the free flow of data and international trade. It also offers some safeguards for children by requiring verifiable parental consent and prohibiting harmful data processing and targeted advertising to children, which protects the vulnerable group.

4.2 Limitations and Concerns

But the DPDP Act has some limitations, especially in the emerging area of artificial intelligence. For instance, the Act does not explicitly address AI, as it does not refer to the risks of automated decision-making, algorithmic bias, or transparency and explainability: thus, the lack of transparency and explainability can potentially expose people to the "black box" profiling. Also, the Act has a wide exemption for government agencies as it permits access to

[23] Constitutionality of the Digital Personal Data Protection Act, 2023, Supreme Court Observer, available at: https://www.scobserver.in/cases/constitutionality-of-the-digital-personal-data-protection-act-2023/

information for purposes such as sovereignty and public order, which can result in unregulated government surveillance, particularly when used with AI technologies such as facial recognition and predictive policing[24].

The Act also does not offer a high level of protection of mass surveillance, while the AI systems may be largely based on the massive data collection, which can enable intrusive surveillance. Also, unlike other laws, such as the GDPR, the DPDP Act does not provide a clear categorisation of data, which treats all personal data equally, which is not appropriate for AI, where some data, such as biometric and health data, will need to be protected at a higher level. Finally, the Act does not provide any direct rights of people to not be subjected to automated decision-making and profiling, which is a significant gap in an AI-driven economy where algorithms have more and more significant influence on key areas of life, including employment, access to credit, and eligibility to the services, and puts people at the risk of being subjected to unfair or discriminatory results.

5. COMPARATIVE GLOBAL APPROACHES

As countries navigate the complexities of artificial intelligence, various jurisdictions have adopted different approaches to AI regulation, depending on their legal, economic and political systems. These global approaches can inform India's efforts to build a robust AI governance framework. From the European Union's comprehensive, rights-based approach to the United States' sector-specific regulations to China's government-led approach, each has its merits and drawbacks, and can inform India's policy landscape.

The European Union has taken a leading role in digital governance with two major regulations: the General Data Protection Regulation (GDPR) and the EU AI Act. The GDPR, which came into force in 2018, is the most stringent data protection regulation globally, focusing on personal data protection and privacy. It provides data subjects with rights, including access, rectification and erasure. The GDPR is also significant for its extraterritorial reach, meaning any company that processes data of EU citizens must comply with the GDPR, regardless of where they are located.

Likewise, the EU AI Act adopts a risk-based approach to regulating AI, categorising systems

[24] Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Act, 2023: Explanatory Note.

based on risk. High-risk systems, such as those used in healthcare, education, or critical infrastructure, must adhere to strict safety, transparency and human oversight requirements, while low-risk systems have minimal requirements. These laws create a multi-faceted governance structure that not only protects personal data but also ensures AI systems are safe, transparent and accountable, with heavy fines for non-compliance.

In contrast, the US follows a sectoral approach to data privacy, with specific regulations for each sector. HIPAA, COPPA, GLBA, FCRA and FERPA govern health, children's data, financial data, credit reporting and education records respectively. Additionally, state regulations, like California's CCPA/CPRA, provide consumers with rights to access, delete, and opt out of the sale of their data [25]. This fragmented approach allows for flexibility and innovation, but also creates complexity and inconsistencies in standards and enforcement across sectors.

By contrast, China adopts a more authoritarian approach with strong government control and regulation. Its AI governance is closely tied to national security, social stability and technological advancement. China's strict algorithm regulations, oversight of generative AI and deep synthesis technologies, and the need to register algorithms and conduct security testing mean that the state has tight control over the functioning of AI systems, particularly those that influence public opinion. Laws such as the Personal Information Protection Law (PIPL) and the Data Security Law also regulate data collection, processing and data transfers, further strengthening state control over data. China also promotes ethical principles like fairness, privacy and accountability, but these are in relation to state objectives. This enables innovation while ensuring regulatory oversight, in line with China's priorities[26].

These cases demonstrate that there is no one size fits all approach to AI governance. These differ in their approach to balancing innovation, regulation and societal priorities, giving India a range of options to draw from as it develops its own balanced, context-specific approach to AI regulation.

6. CASE STUDIES: AI AND THE LAW IN INDIA AND ABROAD

Several court cases have been instrumental in shaping data protection and privacy laws in India

[25] California Consumer Privacy Act, 2018 (USA)
[26] Personal Information Protection Law, 2021 (China)

and elsewhere. In Justice K.S. Puttaswamy v. Union of India (2017)[27], the Supreme Court of India recognised the right to privacy as a fundamental right, laying the foundation for modern data protection laws in India. The case emphasised the importance of principles such as consent, purpose limitation and the need to protect individual autonomy, which were later reflected in the DPDP Act.

The Aadhaar case[28] also raised concerns about large-scale data collection, especially with respect to biometric matching and concerns about data security, misuse and lack of informed consent. It highlighted the responsibilities of data controllers, including the need for effective complaint redressal and consent management, and therefore emphasised the need to safeguard data principals in large-scale digital identity systems [29].

At the international level, the case of Google Spain SL v. Agencia Española de Protección de

Datos (2014) was a landmark ruling in the creation of the "right to be forgotten", which allows individuals to request the removal of inaccurate or irrelevant personal data from search engine results. This case is a good example of the strengthened rights of individuals under the GDPR, such as the right to erasure and objection, compared to the DPDP Act [30].

Similarly, the Schrems II case emphasised the importance of strong safeguards in cross-border data transfers by invalidating the EU-US Privacy Shield for failing to protect EU citizens' data. This case highlights the GDPR's stringent requirements for international data transfers, in contrast to the DPDP Act, which is largely based on executive orders without specific regulations [31].

Finally, the British Airways data breach case demonstrated the GDPR's strong enforcement regime, with the airline facing substantial fines based on its global turnover. This highlights the emphasis on corporate accountability and deterrent effects through proportionate penalties. Although the DPDP Act also provides for significant penalties, these are not based on the company's turnover, which may limit their deterrent effect on large corporations [32].

[27] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[28] Justice K.S. Puttaswamy (Aadhaar) v. Union of India, (2018) 1 SCC 1 (Supreme Court of India).
[29] Ian J. Goodfellow et al., "Explaining and Harnessing Adversarial Examples", Proceedings of the International Conference on Learning Representations (2015)
[30] Google Spain SL v. Agencia Española de Protección de Datos, Case C-131/12 (2014)
[31] Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II), Case C-311/18 (2020)
[32] UK Information Commissioner's Office v. British Airways Plc, Monetary Penalty Notice (2020)

7: LESSONS FOR INDIA

India is at a critical juncture in its AI regulatory journey. India must balance its democracy, diversity and technological innovation with regulation. In this, the European Union and China offer lessons; but India must adapt them to its context.

7.1 Insights from the EU's GDPR and AI Act

The European Union's GDPR and AI Act[33] offer lessons on the balance between rights and ethics in digital regulation, which can be adapted to India. First, there is a need for a risk-based approach to regulation, which categorises AI systems based on their risk, allowing low-risk applications to thrive while high-risk applications, such as in healthcare and critical infrastructure, are more heavily regulated. Additionally, the European model emphasises the need to protect human rights, including privacy, fairness and non-discrimination, which fosters trust and ensures that technological advancement does not come at the cost of human dignity. Transparency and accountability are also key, with transparency about the use of AI and human oversight ensuring that developers and organisations are responsible for their AI systems.

7.2 Insights from China's State-Controlled Approach

China's state-controlled model, despite its different political system, provides lessons on regulatory agility and proactive regulation. Its proactive approach to regulating emerging technologies, such as the swift regulation of generative AI[34], underscores the need for timely action to mitigate risks. Additionally, China's emphasis on aligning AI development with social values implies the importance of incorporating ethical considerations, such as responsible AI, into policies, even in a democratic country like India.

7.3 Adapting the Strategy for India

India's approach must be contextualised to its socio-political and economic environment, and cannot be a replica of either. India, being a diverse democracy with a strong culture of innovation and a diverse population, requires a regulatory and flexible approach. This could involve enacting a framework law that outlines general principles for AI governance, and industry-specific guidelines for areas such as health, finance and education. Encouraging

[33] Council of Europe, Convention 108+: Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (2018)
[34] Human Rights Watch, How AI Could Reinforce Biases in the Criminal Justice System (2022)

selfregulation by industry can also drive innovation and accountability, and strengthening international collaboration will ensure that India's AI policies align with global standards while safeguarding national interests.

8. RECOMMENDATIONS AND FUTURE-PROOF PRIVACY STRATEGIES

As artificial intelligence becomes increasingly embedded in India's digital ecosystem, the question is not whether to regulate it, but how. India must move from reactive to proactive approaches that prioritise privacy, ethics and accountability in AI. Emphasising principles such as privacy by design, transparency and user control[35], India can build a culture of responsible AI that respects individual rights while promoting innovation.

This can be done by adopting privacy by design and by default in AI systems. This means incorporating privacy measures early in the design process, rather than after the fact, to minimise data collection, limit data use, ensure security and transparency in data processing. Privacy by default also supports this by ensuring the most privacy-protecting settings are applied by default (without user intervention), thereby increasing trust and reducing risks.

Likewise, enhancing transparency and explainability in AI systems, which are often "black boxes", is important. Explainable AI decisions include transparency about the use of AI, interpretability tools such as SHAP and LIME, and the ability for humans to understand decisions. This promotes fairness, identifies biases and builds trust in AI.

Consent also needs to be more transparent, robust and user-friendly. India should move away from standardised click-through consent to informed, granular and revocable consent[36] that allows users to know what data is being collected[37], choose how it is used, and modify or withdraw consent through simple interfaces. This helps overcome consent fatigue and user empowerment.

Data governance and security are essential for ethical AI. This includes data quality and integrity, encryption and access control, data ownership and accountability, and audits for compliance and anomaly detection. Data governance minimises risks and enhances trust in AI.

[35] Reserve Bank of India, Guidelines on AI in Banking (2021)
[36] Arindrajit Basu, “Surveillance in the Digital Age: Constitutional Challenges”, 60 Journal of the Indian Law Institute 112 (2018)
[37] Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach, 4th edn. (2021)

Also, India must amend its laws to support AI. While existing laws such as the DPDP Act provide a foundation, further amendments are needed to clarify the rules on accountability and liability for AI-related harm, address concerns of algorithmic bias and discrimination, ensure transparency and explainability for high-risk AI systems, and resolve intellectual property concerns with AI-generated content. These changes must strike a balance between innovation and rights.

Finally, empowering users through greater control and digital literacy is crucial. India needs to focus on education and awareness initiatives to equip individuals with information about AI, its risks and their data rights.[38] By integrating AI literacy into education, training and awareness programs, we can create a more empowered and responsible digital society, equipped to safely and effectively engage with AI technologies.

9. THE FUTURE: PRIVACY IN AN AI-DRIVEN INDIA

India is on the brink of an AI-driven future, in which emerging technologies will transform sectors such as health, education, finance and government, but also pose threats of discrimination, surveillance and abuse.[39] India's privacy laws must be flexible, inclusive and adaptive to succeed in this new world. The path to this future is to focus on ethics in AI development, strengthen legal frameworks, promote international cooperation and empower people through education and control. By pursuing these goals, India can ensure that its AI revolution is not only innovative but also privacy-protecting, rights-enhancing and socially inclusive.

The rapid development of AI also underscores the need for this approach. Multimodal AI, which can process and generate text, images, audio and video, is creating more immersive experiences but also raises privacy concerns due to the amount of personal data involved. Similarly, agentic AI is evolving from automation to systems that can think, plan and learn, presenting new challenges of responsibility and liability.

Generative AI is also being integrated into many industries, enhancing productivity in areas as varied as design and customer service, but also raising concerns about misinformation,

[38] Future of Privacy Forum, Privacy and AI Governance Landscape (2023).
[39] Parliament of India, Department-related Parliamentary Standing Committee on Information Technology, Report on the Personal Data Protection Bill (2021).

intellectual property and data misuse. However, there are still many issues to be addressed, such as data quality and bias, privacy and security, transparency and explainability in decisionmaking, socio-economic effects such as displacement of jobs, and regulatory lag as technology outpaces legislation. Addressing these challenges is crucial to ensure that AI development does not undermine equity, rights and social cohesion.

In this context, there is a need for continuous and participatory policy-making. The speed of AI development means that ad hoc policy interventions are insufficient; India must adopt a dynamic and responsive policy approach to keep up with technological advancements. This can be achieved through consultations with government, industry, academia and civil society to ensure policies are technically robust and socially responsive.

Regulatory sandboxes and pilot projects can allow experimentation in a safe environment, enabling policymakers to test and refine strategies before full-scale roll-out.[40] Regular reviews and updates of legislation are essential to keep up with the times, and international collaboration can help harmonise standards, reduce regulatory costs and allow India to take a leading position in global AI governance. Through this iterative and collaborative process[41], India can build a resilient and sustainable AI ecosystem that promotes innovation while protecting privacy and accountability.

CONCLUSION

The Digital Personal Data Protection Act, 2023 is a good start for privacy in India. However, in the era of Artificial Intelligence, the current laws may not be sufficient as the rise of Artificial Intelligence has introduced new challenges that require more advanced regulation. The Act provides a foundation, but it does not adequately address issues related to AI such as algorithmic bias, automated decision-making and surveillance. Ignoring these issues could jeopardise privacy. Therefore, a more holistic, technology-sensitive legal framework is required to protect privacy while enabling innovation. This requires continuous legal reform, institutional development and engagement. Improving consent, transparency and explainability, and data management are key.

[40] Telecom Regulatory Authority of India, Privacy, Security and Ownership of Data in the Telecom Sector (2018).
[41] Usha Ramanathan, "Aadhaar & Surveillance: Lessons for AI Governance", 8 Indian Human Rights Law Review 56 (2020)

It is also important to be vigilant about emerging risks such as deepfakes, surveillance and autonomous decision-making. Digital literacy will be essential to enable citizens to engage with AI rather than just be impacted by it. Ultimately, India's future should be guided by a simple aspiration: to be the global leader not only in technological capability but also in building a safe, ethical and inclusive AI ecosystem. This can be done through government-industry-academia-civil society partnerships. Only through hard work and ethical practice can India ensure that innovation and human rights go hand in hand, leading to a safe and democratic future with AI.