THE RIGHT TO PRIVACY IN THE AGE OF ARTIFICIAL INTELLIGENCE: A CONSTITUTIONAL ANALYSIS

Sai Ishwarya Siri, Woxsen University.

ABSTRACT

This paper aims to determine whether the Indian Constitution safeguards the right to privacy against the advances of artificial intelligence. Judicial recognition of the right to privacy in the Constitution through the landmark case Justice K.S. Puttaswamy v. Union of India, 2017 has created challenges in addressing novel forms of surveillance and discrimination enabled by AI technologies such as facial recognition, predictive policing, biometric data, decision-making algorithms, and deepfakes. This paper applies a doctrinal, analytical, and comparative methodology to examine the evolution of the jurisprudence on the right to privacy from the cases of M.P. Sharma up to Justice K.S. Puttaswamy v. Union of India, 2017. Furthermore, it analyzes the adequacy of the recently proposed Digital Personal Data Protection Act, 2023 in light of the proportionality test and compares it to the risk-based approach of the EU\u2019s proposed legislation as well as the sectoral privacy framework in the US. The paper argues that despite the progressive interpretation of the Indian Constitution, legislative and enforcement practices leave much to be desired in terms of protecting individual privacy against AI encroachments. It concludes by suggesting the need for a comprehensive AI governance statute that would bridge the existing legal gaps and proposes a set of policy recommendations for consideration.

Keywords: Right to Privacy; Artificial Intelligence; Constitutional Law; Digital Personal Data Protection Act, 2023; Algorithmic Accountability.

1. INTRODUCTION

The Rapid advancement of Artificial Intelligence (AI) has changed the way technology and society work together. AI was only found in academic research and science fiction but now it has become a part of our daily lives. AI affects how we communicate, work, learn, shop, travel and get the services we need. We see AI in virtual assistants, recommendation algorithms, facial recognition systems, healthcare diagnostics, financial technologies and predictive policing. These AI powered technologies are quickly changing the way we make decisions in our daily life. While these changes have made things more efficient, innovative and convenient they have also raised some legal and constitutional concerns especially when it comes to protecting our personal privacy. AI is different from the other traditional technologies because it relies so much on collecting, processing and analysing large amounts of personal data[1]. Our personal data, like our identity, behaviour, online activities, location, financial transactions and biometric characteristics are collected all the time to train intelligence systems and improve their performance. As AI keeps evolving, the way the data is processed has become more advanced. This is helping governments and private companies access individual's lives. While this can be beneficial to society and the economy, it also raises concerns about surveillance, profiling misuse of data and losing our autonomy.

These concerns are especially important in India, where AI is being used more and more in governance, commerce, healthcare, education and financial services[2]. The use of AI by private technology companies and government initiatives like biometric identification, smart surveillance and digital public infrastructure has started a debate about collecting and using personal information. So, we need to look at whether the current constitutional safeguards can protect an individual's privacy in a time when decisions are made based on data.

The Supreme Court of India established the right to privacy as a fundamental right in the case of *K.S. Puttaswamy v. the Union of India*[3] in 2017. This case recognised the right to privacy as a part of the right to life and personal liberty guaranteed under Article 21[4] of the Indian

[1] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).
[2] NITI Aayog, *National Strategy for Artificial Intelligence #AIForAll* (2018).
[3] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[4] The Constitution of India, art. 21.

Constitution. The judgement stated that informational privacy is essential to our freedom in the digital age and that the state has a duty to protect our personal data. Later the government passed the Digital Personal Data Protection Act in 2023[5], which is a big step towards regulating how an individual's personal information is accessed and used. However, this creates challenges that extend beyond traditional notions of privacy and raise questions about whether the existing constitutional and statutory safeguards are sufficient.

Against this backdrop, this study looks at how India's constitutional framework protects the right to privacy in the age of AI. It explores how the concept of privacy has developed and it analyses the challenges posed by AI driven technologies and evaluates whether the current legal framework is adequate. It also undertakes a comparative analysis of how other countries regulate AI and privacy. Through this analysis, this paper seeks to contribute to the discussion about balancing technological innovation with the protection of fundamental rights, in a rapidly changing digital society.

2. LITERATURE REVIEW

The engagement with the right to privacy in India starts with constitutional jurisprudence. M.P. Jain's[6] work on Indian constitutional law traces the contested development of privacy from its initial rejection by the judiciary in *M.P. Sharma v. Satish Chandra*[7] to its slow recognition as an unenumerated right under Article 21.In the aftermath of the landmark nine-judge verdict in *Justice K.S. Puttaswamy (Retd.) v. Union of India,*[8] Gautam Bhatia[9] argues that the judgment's articulation of a four-pronged limitation test - demanding legality, legitimate aim, proportionality, and procedural safeguards constitutes the definitive constitutional standard for evaluating privacy intrusions. Chinmayi Arun[10] has argued further that the Puttaswamy case created a constitutional mandate for data protection that Parliament has been slow to fulfil and AI technologies have since developed within this governance vacuum.

A second body of scholarship has critically engaged with India's legislative response to this mandate. Vrinda Bhandari and Faiza Rahman have argued that the successive drafts of the data

[5] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
[6] M.P. Jain, *Indian Constitutional Law* (8th edn., LexisNexis, 2018) 1312–1320.
[7] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
[8] Supra note 3.
[9] Gautam Bhatia, *The Transformative Constitution* (HarperCollins, 2019).
[10] Chinmayi Arun & Smitha Krishna Prasad, *Towards a Data Protection Framework* (2018).

protection bill moved further away from the rights-protective framework envisioned by the Court, ending up with the Digital Personal Data Protection Act, 2023 – a statute that gives the Statewide exemptions on national security grounds and does not have an independent regulatory authority[11]. These critiques are directly engaged in the paper's assessment of the statutory framework in Chapter VI.

A third body of literature considers the specific intersection of AI and civil liberties in India. Indian law enforcement agencies have used facial recognition technology in public protests, railway stations and border check posts, without legislative authorisation or judicial oversight[12], say researchers at India's Internet Freedom Foundation. Arindrajit Basu and Elonnai Hickok have examined predictive policing tools trained on historically biased crime data, arguing that such systems disproportionately target Dalit, Muslim and other marginalised communities, implicating not just the right to privacy, but the guarantee of equality under Article 14[13]. Indian scholars have drawn on Shoshana Zuboff's wider theoretical frame of surveillance capitalism to place these developments within a global pattern of extraction of behavioural data by State and corporate actors.[14]

The work of comparative scholars has given us useful standards by which to judge India's position. Paul Schwartz and Daniel Solove have contrasted the EU's rights-based data protection approach with the sectoral, market-oriented approach in the United States.[15] In her analysis of the EU Artificial Intelligence Act, 2024 the world's first comprehensive AI-specific regulatory framework Mireille Hildebrandt points out that its risk-based[16] classification model and mandatory oversight by human's requirements are the emerging international standard against which other jurisdictions should be measured.

Yet there is a significant gap in this body of scholarship. Constitutional scholars mapping privacy jurisprudence do not engage systematically with AI-specific threats. DPDP Act, 2023

[11] Internet Freedom Foundation, *India's Digital Personal Data Protection Act, 2023: A Preliminary Analysis* (2023).
[12] Internet Freedom Foundation, *Project Panoptic: Mapping Facial Recognition in India* (2021).
[13] Arindrajit Basu & Elonnai Hickok, *Artificial Intelligence and Inclusion* (Centre for Internet and Society, 2021).
[14] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).
[15] Paul M. Schwartz & Daniel J. Solove, "Reconciling Personal Information in the United States and European Union" (2014) 102 *California Law Review* 877.
[16] Mireille Hildebrandt, "The Artificial Intelligence Act: A Reasoned Overview" (2023) 14(1) *European Journal of Law and Technology*.

has been criticised by data protection scholars without fully anchoring their critique to the Puttaswamy constitutional framework. AI governance scholars have documented harms but have not translated them into coherent constitutional doctrine. This paper seeks to bridge the gaps by presenting a holistic analysis of the Indian constitutional framework in the face of AI-induced privacy threats and evaluating the statutory response and making constitutionally informed recommendations, a question that the extant literature has raised, but not resolved systematically.

3. RESEARCH METHODOLOGY

The present study uses a doctrinal, analytical, and comparative research approach. Doctrinal research is the main method. The paper looks at constitutional provisions, laws, and court decisions as key legal sources. It analyses them based on accepted principles of constitutional interpretation. This method is suitable for a study focused on the adequacy of a legal framework, in contrast to an empirical investigation of social or institutional outcomes.

Using this doctrinal framework, an analytical method assesses whether the current legal system, viewed as a whole, can handle the specific challenges posed by artificial intelligence. This involves identifying gaps, unclear interpretations, and enforcement issues that are not obvious from just reading the relevant provisions. Chapter VI also includes a comparative method, comparing India's legal framework with those of the European Union and the United States. This comparison aims to highlight specific issues in Indian law rather than provide a full account of foreign laws. Primary sources include the Constitution of India[17], the Digital Personal Data Protection Act[18], 2023, the Information Technology Act, 2000[19], Supreme Court decisions, and international documents like the UDHR[20] and ICCPR[21]. Secondary sources feature peer-reviewed articles, monographs, and reports from organisations such as the Internet Freedom Foundation, the Centre for Internet and Society, and NITI Aayog. The study reflects the state of the law as of mid-2025 and does not include empirical data or primary field research.

[17] The Constitution of India.
[18] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
[19] The Information Technology Act, 2000 (Act No. 21 of 2000).
[20] Universal Declaration of Human Rights, adopted 10 December 1948, UNGA Res. 217 A (III).
[21] International Covenant on Civil and Political Rights, adopted 16 December 1966, 999 UNTS 171.

5. CONSTITUTIONAL EVOLUTION OF THE RIGHT TO PRIVACY

5.1 The Meaning and Nature of Privacy

At its core, privacy is the right of individuals to manage information about themselves and to live their lives without unnecessary interference. It includes three connected aspects:

a. Physical privacy, which protects personal space from intrusion;

b. Informational privacy, which controls how personal data is collected, used, and shared; and

c. Decisional autonomy, which ensures individuals can make choices about their own lives without outside pressure.

In the era of artificial intelligence, informational privacy and decisional autonomy face significant and systematic threats.

5.2 International Recognition

Privacy as a human right is recognised in Article 12 of the Universal Declaration of Human Rights[22]. This article forbids arbitrary interference with an individual's privacy, family, home, or correspondence. Article 17 of the International Covenant on Civil and Political Rights[23] supports this by requiring states to provide legal protection against such interference. The Supreme Court of India has consistently held that international treaties ratified by India serve as valuable tools for interpreting the Constitution. This principle was established in *Vishaka v. State of Rajasthan*[24] and has been applied in privacy law. The international framework thus offers a basis and resource for understanding the constitutional right to privacy.

5.3 Evolution Through Indian Jurisprudence

The development of privacy law in India has been a gradual and contested process. In *M.P. Sharma v. Satish Chandra*[25], an eight-judge bench ruled that the Constitution did not guarantee

[22] Universal Declaration of Human Rights, adopted 10 Dec. 1948, UNGA Res. 217 A (III), Art. 12.
[23] International Covenant on Civil and Political Rights, adopted 16 Dec. 1966, 999 UNTS 171, Art. 17.
[24] *Vishaka v. State of Rajasthan*, (1997) 6 SCC 241.
[25] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

a right to privacy, arguing that the the drafters of the Constitution did not include an equivalent of the Fourth Amendment of the U.S. Constitution[26]. A decade later, in *Kharak Singh v. State of Uttar Pradesh*[27], a six-judge bench partially changed this view, with the majority striking down police rules that allowed home visits as violations of personal liberty under Article 21, while stopping short of recognising privacy as a fundamental right.

A broader understanding emerged in *Gobind v. State of Madhya Pradesh*[28], where Justice Mathew, influenced by American constitutional theory, recognised privacy as a right implicit in Articles 19[29] and 21. The ruling stated that specific areas of a person's life such as intimate conduct, family connections, and personal beliefs are constitutionally protected from State intrusion, even without a clear textual guarantee. This "zones of privacy" concept became important in later rulings.

In *R. Rajagopal v. State of Tamil Nadu*[30], the Supreme Court expanded privacy protections to include both State and private actors, stating that the right to privacy is part of the right to life and liberty under Article 21. The Court acknowledged that private individuals, like publishers and media companies, could violate the constitutional right to privacy, raising issues about the horizontal application of fundamental rights against AI companies.

5.4 The Puttaswamy Judgment: A Constitutional Watershed

The key decision came in *Justice K.S. Puttaswamy (Retd.) v. Union of India,*[31] where a nine-judge bench unanimously overturned M.P. Sharma and Kharak Singh, declaring that the right to privacy is a fundamental right tied to Articles 14, 19, and 21 of the Constitution. This ruling is significant for several reasons. First, it recognised informational privacy which is the right to manage personal data as a constitutionally protected interest. Second, it clarified that privacy is not just a negative right against State interference but a positive right that requires the State to create a legal framework for data protection. Third, the Court set out a four-part test for determining when an invasion of privacy is constitutionally permissible: the invasion must (i) be allowed by law; (ii) aim for a legitimate State goal; (iii) be proportional to the intended

[26] U.S. Const. amend. IV.
[27] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[28] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
[29] *The Constitution of India*, art. 19.
[30] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
[31] Supra note 3.

outcome; and (iv) be accompanied by safeguards against misuse.

The later Aadhaar judgment, *Justice K.S. Puttaswamy (Retd.) v. Union of India (2018)*,[32] applied this framework to biometric data and State surveillance. While the majority upheld the core of the Aadhaar scheme, they struck down parts allowing private entities to verify identities through the Aadhaar database, recognising the constitutional limits on using biometric data beyond its intended purpose. This principle is crucial for AI systems that collect and repurpose personal data.

5.5 Articles 14 and 19: Complementary Constitutional Guarantees

The right to privacy does not depend solely on Article 21. Article 14 guarantees equality before the law and equal protection of the laws. This is relevant when AI systems make decisions based on profiling that leads to arbitrary or biased classifications. Such classifications must meet the standards of intelligible differentiation and rational connection, a requirement that unclear algorithmic systems generally cannot fulfill. Article 19(1)(a),[33] which ensures freedom of speech and expression, is affected by AI-enabled surveillance systems that create a chilling effect on public protests, political dissent, and anonymous communication. The constitutional framework thus offers various points of engagement against AI-related privacy threats, serving as a multi-faceted foundation for further analysis in this paper.

6. AI AND EMERGING PRIVACY CHALLENGES

6.1 Facial Recognition Technology

Facial recognition technology poses a significant challenge to the right to privacy in the age of AI. Unlike other identification methods, facial recognition works without consent, from a distance, and on a large scale. This allows the State to identify and track individuals in public spaces without their knowledge. In India[34], these systems have been used at airports, railway stations, public protests, and religious gatherings, often without any legal basis, public privacy assessments, or a way to contest wrongful identification. Applying the Puttaswamy proportionality test, these uses fail at the first step. They are not authorised by any law that ensures legal certainty and predictability. Without a legal framework allowing facial

[32] *Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1.
[33] The Constitution of India, art. 19(1)(a).
[34] Internet Freedom Foundation, Project Panoptic: Mapping Facial Recognition in India (2021).

recognition in public spaces, its use raises constitutional questions under Article 21. Additionally, the chilling effect on assembly and protests engages Article 19(1)(b).[35]

6.2 Predictive Policing and Algorithmic Profiling

Predictive policing systems use AI algorithms trained on past crime data to anticipate criminal activity and direct law enforcement resources. The structural problem lies in the historical crime data, which reflects biased policing rather than actual criminal behaviour patterns. AI systems[36] trained on this data reproduce and worsen existing biases, leading to predictions that unfairly target Dalit, Muslim, tribal, and other marginalised groups. This engages Article 14's guarantee of equality, as algorithmic classification that disadvantages people based on community membership cannot meet the intelligible differentia standard. It also pertains to Article 21, since predictive surveillance subjects individuals to negative outcomes like increased police scrutiny, travel restrictions, or preventive detention without a personalised assessment or due process.

6.3 Biometric Databases and Function Creep

India's Aadhaar system has built the largest biometric database in the world[37]. It links fingerprints and iris scans to a unique ID used for various government services. The constitutional issue, highlighted in the Aadhaar judgment, is function creep: using biometric data collected for one purpose (identity verification for welfare) for other undisclosed reasons, including law enforcement surveillance and AI training. As AI systems increasingly depend on biometric data for identification, authentication, and behavioural analysis, the risk of function creep grows. The principle of purpose limitation considered constitutionally required by the Puttaswamy court, mandates that biometric data collected for statutory reasons cannot be repurposed without new legal authorisation and the individual's informed consent.

6.4 Automated Decision-Making

Automated decision-making systems are AI tools that determine eligibility for credit, jobs, insurance, benefits, or bail without human oversight. These raise serious issues under Article 21's guarantee of fair and reasonable procedures. Denying a benefit or imposing a disadvantage

[35] The Constitution of India, art. 19(1)(b)
[36] Centre for Internet and Society, *Artificial Intelligence and Inclusion* (2021).
[37] Unique Identification Authority of India (UIDAI), About Aadhaar.

based on an algorithm, without an obligation to explain the decision or allow the affected person to challenge it, contradicts the principles of natural justice that the Supreme Court deems inherent in Article 21. Currently, India lacks a legal right to an explanation for automated decisions, creating a stark contrast with Article 22 of the EU General Data Protection Regulation[38] and leaving individuals without legal recourse against algorithmic decisions that impact their basic rights.

6.5 Deepfakes and Generative AI

Generative AI systems that create synthetic images, audio, and video of real people- known as deepfakes pose a new kind of threat to privacy and dignity. Non-consensual deepfake pornography, AI-generated political misinformation[39] linked to real individuals, and synthetic audio for financial fraud have all been reported in India. The constitutional framework addresses these issues through Article 21's protection of dignity, recognised by the Supreme Court as a key part of the right to life, and through Article 19(1)(a), which includes the right to reputation. The specific legal gap lies in the absence of provisions in the DPDP Act, 2023[40], or the IT Act, 2000[41], that directly tackle AI-generated synthetic content involving real individuals without consent.

6.6 Surveillance Capitalism and Data Harvesting

Private AI companies in India collect behavioural data like browsing habits, purchase histories, location data, and social connections on a scale that surpasses State efforts. This data forms detailed individual profiles used to predict and influence behaviour for commercial gain. The constitutional question raised by post-Puttaswamy scholarship is whether fundamental rights also apply to private corporations a question the Court has left somewhat open. The DPDP Act, 2023, addresses this with consent requirements and data fiduciary duties, but its broad exemptions and weak enforcement mechanisms fail to adequately address the constitutional gap. The result is a surveillance system part State, part corporate that the current legal framework cannot effectively regulate.

[38] Regulation (EU) 2016/679 (General Data Protection Regulation), Art. 22.
[39] World Economic Forum, Deepfakes and the Future of Content Integrity (2024).-=
[40] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
[41] The Information Technology Act, 2000 (Act No. 21 of 2000).

7. EXISTING LEGAL FRAMEWORK AND COMPARATIVE ANALYSIS

7.1 The Statutory Framework in India

India's legal approach to data privacy has developed in two phases. The Information Technology Act, 2000 and its Section 43A[42], along with the Sensitive Personal Data or Information Rules, 2011[43], marked the first effort to impose data protection responsibilities on companies handling sensitive personal data. This framework was limited in scope, only addressing electronic records and remaining silent on state actors and artificial intelligence. The Digital Personal Data Protection Act, 2023 represents a more substantial legislative effort. It establishes responsibilities for data minimisation, purpose limitation, and consent for data fiduciaries and creates a Data Protection Board as the adjudicatory authority[44].

However, the Act has serious structural flaws, especially concerning AI. First, Section 17[45] gives the Central Government the power to exempt itself and its agencies from nearly all provisions of the Act, based on broadly defined national security and public order reasons. This exemption contradicts the Puttaswamy proportionality framework, which requires that state intrusions into privacy be legal and necessary. Second, the Act does not specifically address AI systems, automated decision-making, algorithmic profiling, or synthetic media, which are the technologies creating significant privacy threats today. Third, the Data Protection Board has yet to be established, rendering the enforcement framework ineffective. Fourth, NITI Aayog's Principles for Responsible AI[46], while offering helpful policy guidance, are non-binding and lack enforcement mechanisms.

7.2 Comparative Analysis: European Union

The European Union's approach to AI and privacy offers the most comprehensive regulatory framework in existence. The General Data Protection Regulation (GDPR) grants a right to explanation for automated decisions that significantly affect individuals under Article 22. It also requires mandatory data protection impact assessments for high-risk processing, along with an independent supervisory authority in each member state. The EU AI Act, 2024 adds a

[42] The Information Technology Act, 2000, s. 43A.
[43] The Information Technology Act, 2000, s. 43A; The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), 11 April 2011.
[44] The Digital Personal Data Protection Act, 2023, ss. 18–28.
[45] The Digital Personal Data Protection Act, 2023, s. 17.
[46] NITI Aayog, Responsible AI #AIFORALL: Operationalizing Principles for Responsible AI (2021).

risk-based classification of AI systems. Applications in biometric identification, law enforcement, and welfare benefits are considered high-risk and subject to mandatory compliance checks, transparency requirements, human oversight, and restrictions in certain situations, such as real-time biometric surveillance in public spaces. India does not have an equivalent to Article 22 of the GDPR[47] or any risk framework specific to AI.

7.3 Comparative Analysis: United States

The United States has taken a sectoral and market-driven approach. It relies on specific statutes rather than comprehensive federal legislation. The Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI (2023)[48] provides guidelines for federal AI use but has limited legal power. Some states, such as Illinois with the Biometric Information Privacy Act[49] and California with the California Consumer Privacy Act[50], have enacted stronger protections. However, the lack of a unified federal law leads to regulatory inconsistencies. India has a unified data protection law, which is an advantage over the U.S., but it falls short regarding judicial enforcement, algorithmic accountability, and an AI-specific legal framework.

7.4 India's Position

The comparative analysis shows that India is in an intermediate position. It is more advanced than the United States at the federal level in terms of having unified data protection legislation but lags significantly behind the European Union in AI-specific laws, independent oversight, mandatory transparency, and enforceable individual rights against automated systems. The constitutional framework, based on Puttaswamy, offers a stronger basis than either of the other jurisdictions. However, the implementation of legislation is lacking when compared to the constitutional mandate.

8. CHALLENGES, RECOMMENDATIONS AND CONCLUSION

[47] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), art. 22.
[48] Executive Order No. 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (30 October 2023).
[49] Illinois Biometric Information Privacy Act, 740 ILCS 14.
[50] California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199.

8.1 Key Challenges

The analysis in the previous chapters identifies five main challenges facing India's privacy framework in the age of AI. First, there is a legislative gap. The DPDP Act, 2023 discusses personal data processing broadly but lacks provisions targeting AI systems, automated decision-making, or synthetic media. Second, state exemptions allow the government to avoid data protection obligations based on vague reasons that effectively reinstate the pre-Puttaswamy situation of unrestricted state surveillance. Third, algorithmic bias is a concern because there is no statutory requirement to audit AI systems for discriminatory outcomes, which leaves marginalised communities without a way to address AI-driven inequality relevant to Articles 14 and 21. Fourth, there is an enforcement void. The Data Protection Board has not begun operating, and while courts can recognise rights, they often lack the technical expertise and capacity to manage complex algorithmic systems on a case-by-case basis. Lastly, there is a transparency and accountability problem. Current Indian law does not require any entity, public or private, to explain or justify AI-driven decisions that affect individuals.

8.2 Recommendations

The paper suggests five specific recommendations.

a. Parliament should create a dedicated AI Governance Act that includes a risk-based classification system similar to the EU AI Act. This should require human oversight for high-risk AI uses in law enforcement, welfare allocation, and automated decision-making, along with banning real-time biometric surveillance in public spaces without prior judicial approval.

b. Amendments to the DPDP Act, 2023 should either eliminate or significantly limit the state exemptions in Section 17 and introduce a legal right to explanation for automated decisions with major individual impacts.

c. An independent AI and Data Protection Regulator should be set up with financial independence, technical expertise, and enforcement powers. This should be separate from the Data Protection Board as it currently exists and the telecommunications regulatory framework.

d. Courts should explicitly apply the Puttaswamy proportionality test to algorithmic systems, treating lack of clarity and absence of a legitimate aim as serious constitutional flaws.

e. Finally, all public sector AI uses should undergo mandatory algorithmic impact assessments, done independently and made fully available before deployment.

8.3 Conclusion

The right to privacy, recognised in the constitution through Puttaswamy, serves as an important but insufficient foundation for addressing privacy threats posed by artificial intelligence. The constitutional framework, based on Articles 14, 19, and 21, along with the proportionality test, provides a rich basis for challenging AI-driven surveillance, algorithmic bias, automated decision-making without due process, and unauthorised use of biometric and synthetic data. Nonetheless, constitutional acknowledgment without legislative action and proper enforcement remains a goal rather than a reality. The DPDP Act, 2023 is a necessary step but inadequate. It discusses data processing broadly while leaving many specific issues related to AI essentially unregulated. India's position is stronger than the United States regarding legislative unity but much weaker than the European Union in AI governance highlights the urgent need for reform. Privacy in the age of AI is not just a legal issue, it raises questions about whether constitutional democracy can keep pace with technology. The necessary changes, as this paper argues, require vigilant judicial oversight and thoughtful, constitutionally grounded legislative action.

REFERENCES

Cases

1. *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
2. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
3. *Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1.
4. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
5. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
6. *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
7. *Vishaka v. State of Rajasthan*, (1997) 6 SCC 241.

Table of Statutes

India

1. The Constitution of India, 1950, arts. 14, 19, 19(1)(a), 19(1)(b), 21.
2. Digital Personal Data Protection Act, 2023, Act No. 22 of 2023.
3. Information Technology Act, 2000, Act No. 21 of 2000.
4. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), 11 April 2011.

Foreign and International

1. California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199.

2. Executive Order No. 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (30 October 2023).

3. Illinois Biometric Information Privacy Act, 740 ILCS 14.

4. International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171.

5. Regulation (EU) 2016/679, General Data Protection Regulation, art. 22.

6. U.S. Constitution, amend. IV.

7. Universal Declaration of Human Rights, GA Res 217 A (III), 10 December 1948.

Bibliography

1. Arun, Chinmayi, and Smitha Krishna Prasad. *Towards a Data Protection Framework* (2018).

2. Basu, Arindrajit, and Elonnai Hickok. *Artificial Intelligence and Inclusion* (Centre for Internet and Society, 2021).

3. Bhatia, Gautam. *The Transformative Constitution* (HarperCollins, 2019).

4. Hildebrandt, Mireille. "The Artificial Intelligence Act: A Reasoned Overview" (2023) 14(1) *European Journal of Law and Technology*.

5. Internet Freedom Foundation. *India's Digital Personal Data Protection Act, 2023: A Preliminary Analysis* (2023).

6. Internet Freedom Foundation. *Project Panoptic: Mapping Facial Recognition in India* (2021).

7. Jain, M.P. *Indian Constitutional Law* (8th edn, LexisNexis, 2018).

8. NITI Aayog. *National Strategy for Artificial Intelligence: #AIForAll* (2018).

9. NITI Aayog. *Responsible AI: Operationalizing Principles for Responsible AI* (2021).

10. Schwartz, Paul M., and Daniel J. Solove. "Reconciling Personal Information in the United States and European Union" (2014) 102 *California Law Review* 877.

11. Unique Identification Authority of India (UIDAI). *About Aadhaar*.

12. World Economic Forum. *Deepfakes and the Future of Content Integrity* (2024).

13. Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).