Page 3120 - 3132

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

Human Rights in the Age of Artificial Intelligence: With Special Reference to the Right to Privacy

ASHEESH YADAV*

ABSTRACT

The rapid proliferation of artificial intelligence (AI) technologies across governmental, commercial, and social spheres has generated profound tensions with the foundational architecture of human rights law. Among the rights most acutely imperilled is the right to privacy, which occupies a central position in both international human rights instruments and constitutional jurisprudence across the world. This paper examines the multifaceted relationship between AI and the right to privacy, tracing how machine learning systems, mass surveillance infrastructure, facial recognition technologies, and predictive analytics challenge the normative content of privacy as a legal and moral right. It surveys the international human rights framework governing privacy, analyses the constitutional and statutory landscape in India with particular attention to the landmark judgment in K.S. Puttaswamy v. Union of India *and the Digital Personal Data Protection Act, 2023, and engages with comparative regulatory developments, including the European Union's AI Act and the Council of Europe's AI Convention. The paper argues that effective protection of the right to privacy in the age of AI demands not only updated legislation but a rights-by-design approach to AI governance, grounded in the principles of legality, proportionality, accountability, and non-discrimination. It concludes with a set of normative and institutional recommendations.*

Keywords: *Artificial Intelligence, Human Rights, Right to Privacy, Surveillance, Algorithmic Decision-Making, DPDPA 2023, AI Governance, Puttaswamy, Facial Recognition, Data Protection.*

I. INTRODUCTION

The emergence of artificial intelligence (AI) as a pervasive and consequential technology has inaugurated a new chapter in the long history of tensions between technological power and human rights. From mass surveillance to algorithmic profiling, and from autonomous decision-making to the commodification of personal data, AI systems operate at the intersection of

* Author is an Assistant Professor at The ICFAI University, Raipur, Chhattisgarh, India.

 [ISSN 2581-5369]

extraordinary capability and extraordinary risk. Of the many human rights implicated by AI, none is more directly and comprehensively threatened than the right to privacy.

Privacy has long been recognised as a foundational right in the international human rights order. Article 12 of the Universal Declaration of Human Rights declares that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence.[1] Article 17 of the International Covenant on Civil and Political Rights reinforces this protection, obligating states to provide effective legal safeguards against such interference.[2] At the regional level, Article 8 of the European Convention on Human Rights has generated a rich jurisprudence on the permissible limits of state intrusion into private life.[3]

Against this normative backdrop, AI presents a qualitatively new set of challenges. Shoshana Zuboff has theorised the phenomenon as "surveillance capitalism", whereby the behavioural data generated by billions of internet users is harvested, analysed, and monetised as a raw material for prediction products sold in behavioural futures markets.[4] Frank Pasquale has argued that opaque algorithmic systems constitute a "black box society" in which individuals are profiled and classified by systems they cannot see, understand, or contest.[5] Virginia Eubanks has documented how automated systems used in welfare administration disproportionately burden poor and marginalised communities.[6]

For India, these challenges are particularly acute. As home to the world's largest biometric identification system, an ambitious digital public infrastructure agenda, and a rapidly expanding AI sector,[7] India must navigate the promise of AI-driven development against the constitutional imperative to protect fundamental rights, including the right to privacy as recognised by the Supreme Court in *K.S. Puttaswamy v. Union of India*.[8]

This paper proceeds as follows. It first examines the international human rights framework for privacy as it bears on AI. It then surveys the Indian constitutional and statutory landscape, before analysing specific AI-driven threats to privacy and engaging with comparative regulatory developments. The paper then sets out a series of recommendations and concludes.

[1] Universal Declaration of Human Rights art. 12, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).
[2] International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.
[3] European Convention on Human Rights art. 8, Nov. 4, 1950, E.T.S. No. 5.
[4] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 8 (2019).
[5] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3 (2015).
[6] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* 12 (2018).
[7] NITI Aayog, *National Strategy for Artificial Intelligence* 4 (2018), https://niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf.
[8] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

 [ISSN 2581-5369]

II. THE INTERNATIONAL HUMAN RIGHTS FRAMEWORK AND PRIVACY IN THE AGE OF AI

A. Privacy as a foundational human right

Privacy is not merely a personal preference or a cultural value; it is a legally enforceable human right whose content has been developed across decades of treaty practice, judicial decision, and scholarly analysis. The International Covenant on Civil and Political Rights, ratified by 173 states, requires that any interference with privacy be neither arbitrary nor unlawful, and that effective legal remedies be available to those whose privacy rights are violated.[9]

The Human Rights Committee, in its General Comment No. 16, has interpreted the prohibition on arbitrary interference broadly, requiring that any limitation on privacy be proportionate to the specific privacy interest at stake and be accompanied by adequate procedural guarantees. This proportionality requirement is of central importance for AI governance: where AI systems enable surveillance or profiling that goes beyond what is necessary to achieve a legitimate aim, they violate the right to privacy regardless of their technical sophistication.

The Council of Europe's Convention 108+, the first binding international treaty on data protection, establishes core principles for the automated processing of personal data, including the principles of purpose limitation, data minimisation, and individual rights of access and rectification.[10] These principles translate directly into constraints on the design and deployment of AI systems that process personal data.

B. The UN Special Rapporteur and emerging norms

The United Nations Human Rights Council Special Rapporteur on the Right to Privacy has issued a series of reports that apply the international privacy framework to AI-specific contexts. The 2019 report on privacy and AI identified several priority concerns: the opacity of algorithmic decision-making, the aggregation of data from disparate sources to generate inferences to which individuals have never consented, and the deployment of AI in mass surveillance by both state and non-state actors.[11]

The Special Rapporteur has called for the application of human rights impact assessments to AI systems, the prohibition of AI-enabled mass surveillance, and the development of international

[9] International Covenant on Civil and Political Rights art. 17, *supra* note 2.
[10] Council of Europe, Convention 108+ on the Protection of Individuals with Regard to the Processing of Personal Data, May 18, 2018, C.E.T.S. No. 223.
[11] U.N. Human Rights Council, Report of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/HRC/40/63 (Mar. 27, 2019).

 [ISSN 2581-5369]

standards for algorithmic transparency and accountability. While these recommendations remain soft law, they carry significant normative weight and have informed regulatory developments in the European Union, the Council of Europe, and domestic legal systems including India.

C. Business and human rights: corporate responsibility for AI

The UN Guiding Principles on Business and Human Rights establish that corporations have a responsibility to respect human rights, conduct human rights due diligence, and provide or cooperate in remediation where their operations have adverse human rights impacts.[12] Applied to AI developers and deployers, this responsibility framework requires proactive identification of privacy risks in AI systems, the implementation of mitigation measures, and accessible grievance mechanisms for affected individuals.

The application of the Guiding Principles to AI is complicated by the global and distributed nature of AI value chains, in which training data, model development, deployment infrastructure, and end-use may occur across multiple jurisdictions with varying human rights standards. This fragmentation underscores the need for binding international standards rather than reliance on voluntary corporate commitments.

III. Privacy and AI in India: Constitutional and Statutory Dimensions

A. K.S. Puttaswamy v. Union of India: the constitutional anchor

The nine-judge constitutional bench decision in *K.S. Puttaswamy v. Union of India*[13] is the most significant judicial pronouncement on privacy in Indian legal history and provides the constitutional foundation for evaluating AI-related privacy harms. The Court held unanimously that the right to privacy is a fundamental right under Articles 14, 19, and 21 of the Constitution of India, and that it encompasses three dimensions: informational privacy (the right to control personal data), decisional autonomy (the right to make personal choices without state interference), and bodily integrity.

For AI governance, the *Puttaswamy* framework imposes a four-part test for any restriction on privacy: the restriction must be (i) authorised by law, (ii) in pursuit of a legitimate state aim, (iii) proportionate to that aim, and (iv) subject to procedural safeguards.[14] Justice D.Y. Chandrachud's concurring opinion, in particular, articulated a right of informational self-

[12] U.N. Office of the High Comm'r for Human Rights, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, U.N. Doc. HR/PUB/11/04 (2011).
[13] *K.S. Puttaswamy v. Union of India*, *supra* note 8.
[14] *Id.* ¶ 308 (Chandrachud, J., concurring).

 [ISSN 2581-5369]

determination, recognising that individuals must retain meaningful control over data about themselves, including data processed by automated systems.

The *Puttaswamy* judgment was delivered in the context of a challenge to the Aadhaar biometric identification system,[15] but its implications extend far beyond that context. Any AI system that processes personal data, generates inferences about individuals, or enables surveillance must satisfy the *Puttaswamy* tests to be constitutionally permissible. Many existing AI deployments in India, from facial recognition systems used by law enforcement to predictive analytics tools used in welfare administration, have not been subjected to this constitutional scrutiny.

B. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA)[16] is India's first comprehensive data protection legislation and represents a significant step toward giving statutory content to the constitutional right to privacy recognised in *Puttaswamy*. The Act establishes a framework of consent-based data processing, data principal rights, and obligations on data fiduciaries, with direct implications for the governance of AI systems.

The DPDPA grants data principals (individuals whose data is processed) rights of access, correction, erasure, and grievance redress.[17] The Act imposes heightened obligations in respect of children's personal data, prohibiting behavioural monitoring and targeted advertising directed at minors.[18]

The DPDPA nonetheless leaves significant gaps in the governance of AI-specific privacy risks. The Act does not address algorithmic decision-making, automated profiling, or the right to an explanation of automated decisions affecting individuals, provisions that the European Union's General Data Protection Regulation explicitly includes under Article 22.[19] The B.N. Srikrishna Committee, whose 2018 report[20] formed the basis for the data protection legislative process, had recommended provisions on profiling and automated processing, but these were not carried into the final enactment. This legislative gap leaves Indian data subjects without effective legal recourse against AI-driven decisions that affect their rights.

[15] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India).
[16] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[17] The Digital Personal Data Protection Act, 2023, *supra* note 16, §§ 11-13.
[18] *Id.* § 9.
[19] Regulation 2016/679, of the European Parliament and of the Council, art. 22, 2016 O.J. (L 119) 1 (EU) (General Data Protection Regulation).
[20] B.N. Srikrishna Comm., A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics & Information Technology 54 (2018).

 [ISSN 2581-5369]

C. The Information Technology Act, 2000 and existing frameworks

Prior to the DPDPA, the primary statutory protection for data privacy in India was contained in Section 43A of the Information Technology Act, 2000, which imposed liability on corporate bodies for negligent handling of sensitive personal data.[21] This provision was limited in scope, applying only to corporate entities, covering only a subset of personal data, and providing primarily compensatory rather than preventive remedies.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, issued under Section 43A, established baseline security and consent requirements for the processing of sensitive personal data. These Rules have been effectively superseded by the DPDPA, although the transition process is ongoing. Neither the IT Act nor the 2011 Rules addressed AI-specific issues, reflecting the pre-AI vintage of the existing statutory framework.[22]

IV. AI-DRIVEN THREATS TO THE RIGHT TO PRIVACY

A. Mass surveillance and facial recognition technology

Perhaps the most direct AI-driven threat to privacy is the deployment of mass surveillance infrastructure, including facial recognition technology (FRT), CCTV networks integrated with biometric databases, and social media monitoring systems. Unlike traditional forms of surveillance, which require targeted resource deployment, AI-enabled mass surveillance is scalable, continuous, and capable of generating detailed profiles of individuals across time and space.

India has witnessed significant expansion in state surveillance capacity in recent years. Multiple state governments and central law enforcement agencies have deployed or piloted FRT systems, in some cases linked to the national database of criminal records. The Automated Facial Recognition System procured by the National Crime Records Bureau was, in its original tender, proposed to draw on surveillance and police databases for the identification of individuals, raising the prospect of real-time identification without their knowledge or consent.[23]

[21] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 43A.
[22] B.N. Srikrishna Comm., A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics & Information Technology 8-11 (2018) (documenting the inadequacy of the Information Technology Act, 2000 and the 2011 Rules as a data protection framework and the need for dedicated legislation).
[23] Anushka Jain, *NCRB's National Automated Facial Recognition System*, Internet Freedom Found.: Project Panoptic, https://panoptic.in/case-study/ncrbs-national-automated-facial-recognition-system (documenting the National Crime Records Bureau's Request for Proposal for a national Automated Facial Recognition System, its proposed integration with police databases, and the resulting surveillance risks).

 [ISSN 2581-5369]

The deployment of FRT in India raises acute constitutional concerns under the *Puttaswamy* framework. Continuous biometric surveillance in public spaces constitutes a significant interference with informational privacy and decisional autonomy: the knowledge that one is subject to identification and tracking fundamentally alters behaviour, chilling the exercise of rights including free speech and assembly. There is currently no specific statutory authorisation for FRT-based mass surveillance in India, a condition that the *Puttaswamy* legality requirement renders constitutionally suspect.[24]

Constitutional litigation challenging FRT has been initiated, most notably India's first legal challenge to the deployment of FRT, filed as a public interest litigation in the Telangana High Court,[25] but such proceedings remain pending, and the absence of interim relief has allowed deployment to continue. The lack of judicial clarity on the constitutional permissibility of FRT, combined with legislative inaction, has created a rights vacuum in which surveillance capacity expands without commensurate legal constraint.

B. Algorithmic profiling and inference

Beyond direct surveillance, AI systems threaten privacy through the aggregation and inference of personal information from seemingly innocuous data points. A credit scoring algorithm may infer an individual's health status, political affiliation, or religious beliefs from their financial transaction history. A social media recommendation engine may construct a detailed psychological profile from patterns of engagement that the individual has never consciously disclosed.

This inferential dimension of AI poses a distinctive challenge to traditional data protection frameworks, which are predicated on the concept of data that individuals knowingly share. Mireille Hildebrandt has described this as the problem of "data-driven agency", whereby AI systems attribute characteristics and propensities to individuals on the basis of patterns identified across aggregated datasets, characteristics that the individual may not possess, may not know have been attributed to them, and may have no practical means to contest.[26]

---

[24] Internet Freedom Found., Project Panoptic (documenting that live facial recognition deployments in India, including the National Automated Facial Recognition System, operate without any anchoring statutory framework authorising or regulating their use).

[25] *S.Q. Masood v. State of Telangana*, Pub. Interest Litig., High Court of Telangana (notice issued Jan. 3, 2022) (pending) (India) (challenging the deployment of facial recognition technology by the State as lacking statutory authorisation and being disproportionate); *see* Internet Freedom Found., *Telangana High Court Issues Notice in India's First Legal Challenge to the Deployment of Facial Recognition Technology* (Jan. 4, 2022), https://internetfreedom.in/telangana-high-court-issues-notice-in-indias-first-legal-challenge-to-the-deployment-of-facial-recognition-technology/.

[26] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* 65 (2015).

 [ISSN 2581-5369]

The problem of algorithmic bias further compounds privacy harms: where inference algorithms are trained on historically biased data, they may produce inferences that are both inaccurate and discriminatory, violating the right to privacy in conjunction with the right to non-discrimination. Research has documented how facial recognition systems perform significantly less accurately for darker-skinned women than for light-skinned men,[27] and how crime prediction algorithms systematically over-predict recidivism risk for Black defendants.[28]

C. Predictive analytics in criminal justice and welfare

The use of AI in criminal justice and welfare administration represents a domain of particularly serious privacy and rights violations. Algorithmic risk assessment tools such as COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) have been used in the United States to assist sentencing decisions, with the Wisconsin Supreme Court in *State v. Loomis*[29] holding, controversially, that their use does not violate due process provided that courts do not rely on them as determinative.

The investigative journalism outlet ProPublica documented that COMPAS assigned higher recidivism risk scores to Black defendants than to white defendants with comparable criminal histories,[30] illustrating how algorithmic systems can entrench and amplify structural discrimination under the guise of neutral, data-driven objectivity. Where such tools are deployed without disclosure to affected individuals, they also violate informational privacy, since individuals are profiled by systems of which they are unaware, on the basis of data they have not consented to share.

In India, AI tools are increasingly being piloted in welfare administration, law enforcement, and border management. The absence of a specific legal framework for algorithmic decision-making in these high-stakes contexts means that individuals affected by adverse AI-driven decisions have limited recourse under existing law,[31] a situation that is inconsistent with constitutional guarantees of equality, due process, and privacy.

D. Data brokers, commercial AI, and the commodification of personal data

The commercial AI ecosystem poses a different but equally serious set of privacy threats. The business models of major technology platforms are built on the continuous collection, analysis,

[27] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RES. 77, 81 (2018).
[28] Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[29] *State v. Loomis*, 881 N.W.2d 749, 753 (Wis. 2016).
[30] Angwin et al., *supra* note 28.
[31] Rishab Bailey & Vrinda Bhandari, *Regulatory Challenges of AI in India*, Centre for Internet & Society 12 (2022).

 [ISSN 2581-5369]

and monetisation of personal data, including data about health, location, political views, sexual orientation, and financial behaviour. The inference of sensitive attributes from non-sensitive data, and the sale of these inferences to advertisers, insurers, employers, and political actors, constitutes a systematic violation of informational privacy at scale.[32]

The DPDPA attempts to address some of these harms through its consent mechanism and data principal rights, but significant gaps remain, particularly in the regulation of non-personal or anonymised data, which AI systems can often re-identify through inference. The proposed Non-Personal Data Governance Framework, which would govern data that does not identify individuals, remains unpublished as of this writing, leaving an important regulatory gap in AI-specific data governance.[33]

V. COMPARATIVE REGULATORY DEVELOPMENTS

A. The European Union: AI Act and GDPR

The European Union has developed the world's most comprehensive regulatory framework for AI, consisting of the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act), which entered into force in 2024.[34]

The GDPR directly addresses AI-specific privacy concerns through Article 22, which grants individuals the right not to be subject to a decision based solely on automated processing where that decision produces legal or similarly significant effects.[35] This right to human review of automated decisions, combined with rights of access, rectification, and erasure, and the requirement for data protection impact assessments for high-risk processing, provides a robust framework for AI privacy governance that has no direct equivalent in Indian law.

The AI Act adopts a risk-based approach, classifying AI systems into four risk categories and imposing graduated obligations accordingly. AI systems used for mass biometric surveillance, social scoring, and real-time biometric identification in public spaces are prohibited or heavily restricted under the Act. High-risk AI systems, including those used in critical infrastructure, law enforcement, migration, and the administration of justice, must undergo conformity assessment, maintain technical documentation, and comply with transparency and human oversight requirements. This risk-tiered architecture provides a model for India's own AI regulatory design.

---

[32] Smriti Parsheera, *AI and the Right to Privacy in India*, Centre for Internet & Society (Working Paper, 2022).
[33] Smriti Parsheera, *supra* note 32.
[34] Regulation 2024/1689, of the European Parliament and of the Council, 2024 O.J. (L 2024/1689) (EU) (Artificial Intelligence Act).
[35] Regulation 2016/679, *supra* note 19, art. 22.

 [ISSN 2581-5369]

B. Council of Europe Framework Convention on AI

In 2024, the Council of Europe adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, the first binding international treaty on AI.[36] The Convention requires parties to ensure that AI systems under their jurisdiction respect human rights, democracy, and the rule of law, and to implement measures to prevent and remediate AI-induced human rights violations. It explicitly addresses the risks of AI to privacy and data protection, and requires parties to impose specific obligations on private actors in addition to public authorities.

India is not a party to the Council of Europe and is therefore not bound by this Convention. However, as a UN member state that has endorsed the 2024 UN General Assembly resolution on AI and sustainable development,[37] India has committed to advancing safe, secure, and trustworthy AI in accordance with international human rights standards. This commitment creates a normative expectation, if not a legally binding obligation, that India's domestic AI governance framework will align with the standards embodied in the Convention.

C. The OECD AI Principles

The OECD AI Principles, adopted in 2019 and subsequently endorsed by the G20,[38] establish five values-based principles for the responsible stewardship of trustworthy AI: inclusive growth and sustainable development; human-centred values and fairness; transparency and explainability; robustness, security, and safety; and accountability. India, as a member of the OECD AI Policy Observatory and a G20 state, has endorsed these principles, which provide a non-binding but authoritative reference point for domestic AI governance.

The principles of transparency and explainability are of particular relevance to AI and privacy: where individuals cannot understand how AI systems process their data or make decisions about them, they cannot effectively exercise their rights of access, correction, or contestation. Embedding explainability requirements in Indian AI law is therefore not merely a technical nicety but a prerequisite for meaningful privacy protection in the age of AI.

[36] Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, C.E.T.S. No. 225 (May 17, 2024).
[37] G.A. Res. 78/311, Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development (Mar. 21, 2024).
[38] Org. for Econ. Co-operation & Dev., Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 22, 2019).

 [ISSN 2581-5369]

VI. RECOMMENDATIONS

A. Enact an AI-specific privacy framework

India should enact comprehensive AI-specific provisions, either as an amendment to the DPDPA or as a standalone AI governance statute, that address the distinctive privacy risks of AI systems. At a minimum, such provisions should include a right to explanation for consequential automated decisions; mandatory algorithmic impact assessments for high-risk AI systems; transparency requirements for the use of personal data in AI training; and specific restrictions on AI-enabled mass surveillance, including a statutory basis requirement for any biometric identification system operating in public spaces.

B. Operationalise the Puttaswamy framework

The four-part *Puttaswamy* test, requiring legality, a legitimate aim, proportionality, and procedural safeguards, should be operationalised into a statutory framework for AI deployment by state actors. Any government AI system that processes personal data or makes decisions affecting individuals should be required to demonstrate compliance with each element of the *Puttaswamy* test through a published, independently reviewed impact assessment. Judicial review of AI-enabled state action should be actively promoted through updated standing rules and the development of specialised AI adjudication capacity.

C. Establish an independent AI regulatory authority

India currently lacks an independent AI regulatory authority with cross-sectoral jurisdiction, the technical expertise to evaluate complex AI systems, and the legal powers to investigate, sanction, and require remediation. An AI regulatory authority should be established with a statutory mandate that includes the protection of human rights, and in particular privacy, as an explicit and primary objective. The authority should be independent of both the executive branch and industry, adequately resourced, and empowered to issue binding guidance, conduct audits, and impose meaningful penalties for non-compliance.

D. Prohibit high-risk AI applications without adequate safeguards

Following the model of the EU AI Act, India should prohibit, or impose a moratorium on, the deployment of AI systems that pose unacceptable risks to human rights, including real-time biometric surveillance of public spaces in the absence of specific statutory authorisation and independent oversight, social scoring systems that aggregate individual data to produce composite rankings, and AI systems in criminal justice that operate without human oversight or

 [ISSN 2581-5369]

individualised explanation. The deployment of FRT by law enforcement should be regulated by specific legislation that incorporates the *Puttaswamy* proportionality requirements.[39]

E. Adopt a rights-by-design approach

Privacy protection in the age of AI cannot be achieved by ex post legal remedies alone; it requires that rights protection be built into the design and architecture of AI systems from the outset. India should adopt regulatory requirements for privacy-by-design in AI development, including data minimisation, purpose limitation, differential privacy techniques, and federated learning approaches that reduce the need to centralise sensitive personal data. The NITI Aayog's Responsible AI principles[40] should be given statutory backing and translated into concrete technical and organisational requirements.[41]

VII. Conclusion

The age of artificial intelligence is also an age of unprecedented privacy vulnerability. The technologies that promise to transform healthcare, education, agriculture, and governance also enable forms of surveillance, profiling, and manipulation that strike at the core of human dignity and autonomy. The right to privacy, as a cornerstone of the international human rights order and a fundamental right under the Indian Constitution, provides both the normative framework and the legal tools for evaluating and constraining these threats.

India's response to the AI-privacy challenge has been substantive but incomplete. The *Puttaswamy* judgment provides a constitutionally robust framework, and the Digital Personal Data Protection Act, 2023, marks a significant legislative advance. However, the absence of AI-specific privacy protections, including rights of explanation, algorithmic impact assessment requirements, and clear restrictions on biometric mass surveillance, leaves a significant gap between constitutional aspiration and legal reality.

Internationally, the European Union's AI Act and GDPR, the Council of Europe's AI Convention, and the UN General Assembly's AI resolution collectively signal the emergence of a global consensus on the need for rights-based AI governance. India, as a leading AI power and a constitutional democracy committed to fundamental rights, has both the opportunity and the obligation to contribute to this emerging order by developing a domestic framework that is at once technically sophisticated, institutionally robust, and uncompromisingly protective of the dignity and privacy of every person subject to its jurisdiction.

---

[39] Rishab Bailey & Vrinda Bhandari, *supra* note 31.
[40] NITI Aayog, Responsible AI for All: Approach Document for India, Part I 22 (2021).
[41] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. Rev. 399, 430 (2017).

 [ISSN 2581-5369]

The governance choices made in the next legislative cycle will shape not only the trajectory of AI in India but the meaning of privacy, equality, and freedom in an algorithmically mediated society. The jurisprudential and legislative tools exist; what is required is the political will to deploy them in the service of human rights.

*****

 [ISSN 2581-5369]