ARTIFICIAL INTELLIGENCE AND THE RIGHT TO PRIVACY: A CONSTITUTIONAL CHALLENGE FOR INDIA

Sonali Aggarwal, Assistant Professor at MVN University Palwal

ABSTRACT

Artificial Intelligence (AI) has become a defining feature of India's digital transformation, reshaping governance, finance, healthcare, and everyday life. While these innovations promise efficiency and inclusion, they also create unprecedented risks for the constitutional right to privacy. The Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* was a landmark, but translating that principle into practice has proven difficult in the age of big data and algorithmic decision-making.

This paper traces the constitutional journey of privacy in India, from its early denial in *M.P. Sharma* and *Kharak Singh* to its emphatic affirmation in *Puttaswamy*. It then explores how AI threatens privacy through opaque decision-making, algorithmic discrimination, and mass surveillance, often in ways that disproportionately affect vulnerable communities. The analysis critiques India's current regulatory framework—the Digital Personal Data Protection Act, 2023, the pending Digital India Act, and NITI Aayog's policy strategies—highlighting their gaps in algorithmic accountability and institutional independence.

Drawing on comparative jurisprudence from the EU, U.S., China, and the UK, the paper argues that India must adopt a rights-first approach that combines strong constitutional safeguards with practical measures: algorithmic transparency, independent oversight, privacy-enhancing technologies, and citizen empowerment. Ultimately, it concludes that India's aspiration to be a global AI leader must be matched by a parallel commitment to democratic values, ensuring that technological progress strengthens rather than undermines liberty, dignity, and equality.

Keywords: Artificial Intelligence, Privacy, Constitution of India, Fundamental Rights, Data Protection, AI Ethics.

1. INTRODUCTION

Artificial Intelligence (AI) has quickly moved from being a futuristic concept to an everyday reality. In India, algorithms already decide how we access welfare schemes, manage our money, navigate cities, and even how the State polices us. The promise is enormous: AI can make governance smoother, healthcare more accessible, and financial transactions effortless. Yet, the very tools that empower citizens can also endanger them. What happens when the same data used to deliver subsidies is repurposed for surveillance? What if an algorithm misreads your digital footprint and labels you "high risk," shutting you out of opportunities without any chance of appeal?

These questions sit at the heart of India's constitutional debate on privacy. In 2017, the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* declared that privacy is intrinsic to life and liberty under Article 21 of the Constitution.[1] But recognition on paper is only the beginning. As AI systems increasingly process our biometrics, financial trails, and behavioural data, the challenge lies in whether the Constitution—and the institutions that safeguard it—can meaningfully protect citizens in practice.

India's own digital transformation makes this issue particularly urgent. The **Aadhaar project**, the world's largest biometric identity system, has linked millions to welfare benefits and banking services, but has also sparked concerns about profiling and exclusion.[2] The **Digital India campaign** has digitised governance and everyday services, while innovations like **Unified Payments Interface (UPI)** have revolutionised financial transactions, recording billions of transfers every month.[3]Platforms such as **DigiLocker** make document storage seamless, and the **Smart Cities Mission** integrates AI-driven surveillance and predictive traffic systems into urban life.[4] Together, these initiatives illustrate the rapid entrenchment of AI into the Indian state and economy.

But India also faces unique vulnerabilities. Public awareness of privacy rights remains low, especially in rural and semi-urban areas where digital literacy is limited. Regulatory

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[2] Usha Ramanathan, *Aadhaar: From Welfare to Surveillance*, 9 Indian J. Const. L. 1, 5–8 (2015).
[3] National Payments Corporation of India, *UPI Product Statistics*, NPCI (2024), https://www.npci.org.in/statistics/upi-statistics
[4] Ministry of Housing & Urban Affairs, Government of India, *Smart Cities Mission Statement and Guidelines* (2017).

institutions—though formally in place—often lack independence, resources, or technical expertise to enforce privacy rights effectively.[5] Socio-economic disparities mean that the poor and marginalised are more likely to be subject to intrusive surveillance, algorithmic profiling, or data misuse, and less likely to challenge such violations in court.[6] In other words, while the Constitution recognises privacy as a fundamental right, its protection remains fragile on the ground.

This paper therefore asks: Can India's constitutional framework and emerging legal instruments safeguard privacy in an AI-driven era? To answer this, the discussion proceeds in stages: tracing the evolution of privacy as a constitutional right, examining AI's sectoral impact on privacy, critiquing India's regulatory landscape, and drawing lessons from global models. Ultimately, the argument advanced is that India must adopt a **rights-first approach to AI governance**—one that ensures technological progress does not come at the cost of dignity, liberty, and democratic accountability.

2. THE CONSTITUTIONAL RIGHT TO PRIVACY IN INDIA

Privacy was not born in India's Constitution overnight—it has been carved out slowly, case by case, judgment by judgment. The journey begins in the early years of the Republic, when the very idea of privacy seemed alien to constitutional interpretation.

The first stop was *M.P. Sharma v. Satish Chandra* (1954), where an eight-judge bench examined whether search and seizure powers violated a "right to privacy." The Court's answer was blunt: no such right existed under the Constitution. Unlike the U.S. Fourth Amendment, India's framers had not explicitly guaranteed privacy, and the Court declined to read it in.[7]

A decade later, the Court revisited the question in *Kharak Singh v. State of Uttar Pradesh* (1962). Here, the issue was surveillance of a suspect through "domiciliary visits." The majority opinion once again refused to acknowledge a distinct right to privacy. Yet, Justice Subba Rao's famous dissent rang with a different tune: he argued that privacy was an essential part of

[5] Ananth Padmanabhan, *The Illusion of Consent in India's Data Protection Regime*, Centre for Policy Research (2023).
[6] Vrinda Bhandari & Renuka Sane, *Towards a Rights-Respecting Data Protection Law in India*, NIPFP Working Paper No. 408 (2021).
[7] *M.P. Sharma v. Satish Chandra*, 1954 SCR 1077.

personal liberty under Article 21. Although a minority view at the time, Subba Rao's words planted a seed that would later grow into constitutional doctrine.[8]

That seed began to take root in *Gobind v. State of Madhya Pradesh* (1975). While the Court upheld certain forms of police surveillance, it also made a cautious but significant move: it recognised privacy as a fundamental right, albeit one subject to "reasonable restrictions." Justice Mathew observed that privacy was integral to liberty and dignity, and that any intrusion must be justified by a compelling State interest. This was the Court's first real step towards embracing privacy within the fold of fundamental rights.[9]

The next milestone came in *People's Union for Civil Liberties (PUCL) v. Union of India* (1997)—better known as the "telephone tapping case." Here, the Court was asked whether the State could intercept calls without violating rights. It ruled that unauthorised telephone tapping indeed infringed Article 21, and it laid down procedural safeguards, including review committees and prior authorisation requirements, to prevent arbitrary intrusions.[10] This was a turning point: privacy was no longer just a theoretical value but an enforceable right capable of constraining State power.

Finally, in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), a nine-judge bench settled the debate once and for all. The Court unanimously held that privacy is intrinsic to life and liberty under Article 21, overruling *M.P. Sharma* and the majority in *Kharak Singh*. It defined privacy in three dimensions: bodily privacy, decisional autonomy, and informational privacy. Most importantly, the judgment recognised that in a digital age, protecting informational privacy was crucial to preserving dignity and liberty.[11]

Taken together, these cases show a remarkable constitutional journey: from denial, to dissent, to cautious recognition, to full affirmation. Privacy in India has evolved as a living doctrine—moulded by social change, judicial imagination, and the challenges of modern governance. But this evolution also underscores a deeper truth: a right declared in court does not automatically translate into protection on the ground. That gap between recognition and enforcement becomes especially stark in the age of AI, where technology tests the limits of constitutional

[8] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[9] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
[10] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.
[11] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

promises every single day.

3. THE RISE OF AI AND ITS IMPACT ON PRIVACY

Artificial Intelligence thrives on one thing above all else: data. The more data it consumes, the smarter and more accurate it becomes. In India, this means that every click, payment, medical record, or biometric scan can potentially feed into an algorithm. While this data-driven revolution brings efficiency and innovation, it also creates new risks for the right to privacy. To truly understand the challenge, it helps to look at how AI is being used across different sectors.

Healthcare.

AI promises life-saving breakthroughs in diagnosis and treatment. Algorithms can scan X-rays faster than radiologists, predict outbreaks, and personalise care plans. But these systems need vast amounts of sensitive health data—genetic records, prescriptions, hospital histories. What happens when such data is shared across private companies without patient knowledge? Imagine a cancer patient whose medical records are quietly sold to an insurer, leading to higher premiums or outright denial of coverage. Without strict rules of purpose limitation and patient consent, informational privacy in healthcare remains at risk.[12]

Banking and Finance.

India's digital economy now runs on AI. The **Unified Payments Interface (UPI)** processes billions of transactions monthly, and fintech platforms use AI to decide who gets credit and at what rate. In theory, this expands financial inclusion. In practice, algorithms sometimes rely on proxies—like location, online behaviour, or even phone battery usage—to judge "creditworthiness."[13] For someone from a marginalised background, this could mean being unfairly tagged as a "risk" and denied a loan. The worst part? The algorithm offers no explanation, and the individual has no meaningful way to challenge the decision.

Policing and Surveillance.

Perhaps the most troubling use of AI in India lies in law enforcement. Cities are increasingly

[12] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[13] NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll* (2018).

deploying **facial recognition systems** under initiatives such as the National Automated Facial Recognition System (AFRS).[14] On paper, these tools are meant to catch criminals or trace missing persons. But in reality, they also create the possibility of mass surveillance. At a peaceful protest, for instance, facial recognition cameras can identify and catalogue participants, creating a chilling effect on the constitutional rights to free speech and association. When algorithms misidentify individuals—something that often happens disproportionately to women and minorities—the consequences can be devastating.

Workplace and Education. Employers and universities are also turning to AI. Companies use monitoring tools to track employee productivity through keystrokes and screen time, while universities experiment with AI-driven proctoring during online exams. These technologies, though efficient, blur the line between oversight and intrusion. Consent becomes meaningless when workers or students have little choice but to agree. Such constant digital surveillance erodes not only privacy but also dignity and trust.[15]

Social Media and Deepfakes. A newer challenge comes from generative AI. Deepfakes—synthetic videos and audio—can create hyper-realistic but false content. In India, women have been particular targets of non-consensual deepfake pornography, which spreads rapidly across platforms before takedown requests can even be processed. Victims often face lasting reputational harm, with little recourse.[16] Beyond individual harms, deepfakes also threaten democratic processes, fuelling misinformation during elections or public debates.

Across all these sectors, a pattern emerges. AI is not inherently harmful; its risks come from how it is deployed, who controls the data, and what safeguards exist. In India, where digital literacy is low and regulatory institutions are weak, these risks are magnified. Consent forms are often written in complex legal language, oversight bodies lack teeth, and ordinary citizens rarely have the means to challenge algorithmic injustice. The result is a privacy regime that looks strong on paper but feels fragile in practice.

4. LEGAL AND REGULATORY LANDSCAPE IN INDIA

When the Supreme Court in *Puttaswamy* declared privacy a fundamental right, it effectively

[14] Vidushi Marda & Shivangi Narayan, *Facial Recognition Technology in India: A Threat to Privacy and Civil Liberties*, Internet Freedom Foundation (2020).
[15] OECD, *Recommendation of the Council on Artificial Intelligence* (2019).
[16] Apar Gupta, *Deepfakes and the Indian Legal System: Gaps and Challenges*, Internet Democracy Project (2023).

handed the ball to the legislature: build a law that protects people's data in the digital age. India's response came, after years of debate, in the form of the **Digital Personal Data Protection Act, 2023 (DPDPA)**. On paper, it looks like a milestone. In practice, it leaves troubling gaps—especially in the age of Artificial Intelligence.

Scope and Rights. The DPDPA gives Indian citizens—called "data principals"—basic rights: to access their data, correct errors, request erasure, and even nominate someone to exercise these rights on their behalf.[17] It also prohibits tracking and targeted advertising directed at children, a recognition of how vulnerable minors are to digital manipulation.[18] In many ways, this framework mirrors the global trend set by the European Union's GDPR.

Consent Model. The Act is built around consent: processing must be based on free, specific, informed, and unambiguous agreement.[19] To make this workable, it introduces a novel concept—**"consent managers."** These are third-party platforms, registered with the Data Protection Board of India (DPBI), which can manage consents on behalf of individuals. In theory, this innovation empowers citizens. But its success will depend on whether these managers are truly interoperable, independent, and accessible to India's diverse population.

Exemptions for the State. Here lies the Act's most controversial feature. Entire classes of processing can be exempted when done in the name of "sovereignty," "public order," or "security of the state."[20] Even government schemes providing subsidies or benefits are exempt from consent requirements. Imagine a welfare recipient whose biometric data is collected for subsidy delivery; the same data could potentially be repurposed for policing or profiling, without their knowledge or approval. In effect, the very communities that most rely on state benefits become most vulnerable to state surveillance.

Critique: Weak Algorithmic Accountability. The DPDPA was not written with AI in mind. It contains no requirements for algorithmic transparency, fairness audits, or rights against automated decision-making. Unlike the GDPR, there is no "right to explanation" when an AI system denies you a loan, a job, or access to services.[21] In an era where algorithms silently

[17] Digital Personal Data Protection Act, No. 22 of 2023, § 13 (India).
[18] Id. § 9.
[19] Id. § 6.
[20] Id. § 17.
[21] See *Summary of the Digital Personal Data Protection Act, 2023*, Medianama (Aug. 2023), https://www.medianama.com/2023/08/223-summary-india-digital-personal-data-protection-bill-2023

shape opportunities, this silence in the law is deafening.

Weak Enforcement. The Data Protection Board of India is the enforcement body. But here too, independence is in doubt: appointments are made by the central government, raising questions about its ability to act against state actors.[22] Penalties—up to ₹250 crore for each violation—sound impressive, but without investigative teeth and technical capacity, enforcement risks being symbolic rather than substantive.

The Pending Digital India Act. Recognising these shortcomings, the government has proposed a broader **Digital India Act (DIA)** to replace the outdated IT Act of 2000. The DIA promises to regulate online harms, algorithmic accountability, and platform governance.[23] Draft consultations suggest it could impose stricter duties on high-risk AI systems, including transparency and safety requirements. But as of now, the Act remains in draft stage, and its direction is unclear. Critics worry that it may replicate the same pattern—granting sweeping powers to the executive without strong checks and balances.[24]

NITI Aayog's AI Strategy. In parallel, India's policy think tank NITI Aayog has been shaping AI discourse. Its **National Strategy for Artificial Intelligence (2018)**, branded "#AIforAll," focused on economic growth, applying AI in agriculture, healthcare, education, and smart cities.[25] Later, in 2021, it released **Principles for Responsible AI**, emphasising fairness, transparency, and accountability.[26] These are welcome steps but are purely advisory. There are no binding obligations on government agencies or private corporations to follow them. The approach remains innovation-first, rights-later—a dangerous stance in a country where institutions are already struggling to enforce privacy protections.

In short, India has taken important steps toward data protection, but the current legal landscape remains patchy. The DPDPA creates a baseline of privacy rights, but with broad state exemptions and little attention to algorithmic accountability. The DIA could be a chance to fill these gaps, yet its trajectory is uncertain. Meanwhile, soft-law strategies from NITI Aayog offer

[22] See *Personal Data Protection Act 2023: A Step Forward or a Threat to Privacy?*, Lawful Legal, https://lawfullegal.in/personal-data-protection-act-2023-a-step-forward-or-a-threat-to-privacy
[23] *Questions Arise on Digital India Act, Other Tech Regulations in Coalition Govt*, Livemint (June 17, 2024), https://www.livemint.com/technology/questions-arise-on-digital-india-act-other-tech-regulations-in-coalition-govt-11717679193556.html
[24] *India's Proposed Digital India Act Raises Concerns Over State Powers*, Financial Times (July 2024), https://www.ft.com/content/3400d1d3-7fce-4932-b4d3-17a98323f3df
[25] NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll* (2018).
[26] NITI Aayog, *Principles for Responsible AI* (2021).

principles without enforcement. The result is a paradox: India is pushing forward as a global hub for AI while its legal framework to regulate AI's risks remains fragile and incomplete.

5. COMPARATIVE JURISPRUDENCE AND GLOBAL AI REGULATION

India is not alone in grappling with the privacy challenges of Artificial Intelligence. Around the world, governments are experimenting with different legal models to manage AI—some placing human rights at the centre, others prioritising innovation or state control. A comparative look reveals four dominant approaches: the European Union's rights-first framework, the United States' fragmented regulatory patchwork, China's state-driven control, and the United Kingdom's adaptive, pro-innovation stance. Each holds lessons—and warnings—for India.

European Union: Rights Above All.

No region has gone as far as the EU in placing rights at the heart of AI regulation. The **General Data Protection Regulation (GDPR)** already guarantees citizens robust rights: to access their data, demand erasure, or challenge misuse. Building on that foundation, the **EU AI Act** adopts a risk-based model. It outright bans AI practices deemed "unacceptable," such as social scoring or real-time biometric surveillance in public spaces.[27] High-risk systems—like those used in law enforcement or healthcare—must comply with strict safeguards, including transparency, human oversight, and detailed documentation.[28] The EU's message is clear: AI must serve democracy, not undermine it. For India, this model demonstrates that strong regulation and technological growth can coexist if rights are treated as non-negotiable.

United States: Patchwork and Pragmatism.

In contrast, the U.S. has avoided a sweeping national law. Instead, it relies on sectoral regulation and agency-led guidelines. For instance, the Federal Trade Commission applies consumer protection principles to AI, while state-level laws such as California's CCPA fill in privacy gaps.[29] Recently, President Biden's executive orders have also called for testing and auditing high-risk AI systems, though these measures lack the force of comprehensive legislation.[30] This patchwork allows flexibility and fosters innovation, but it creates uneven

[27] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).
[28] European Commission, *The Artificial Intelligence Act* (2024).
[29] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 (2018).
[30] Exec. Order No. 14,110, 3 C.F.R. (2023) (U.S.) (on AI safety and testing).

protection: a citizen's ability to challenge algorithmic harms often depends on which state they live in. For India, the U.S. experience is a reminder that decentralisation can spark innovation but risks leaving citizens vulnerable without a uniform baseline of rights.

China: State-Controlled Deployment.

China represents perhaps the starkest contrast. AI is deeply embedded in state governance, from surveillance cameras to social credit experiments. Regulations on generative AI and recommendation algorithms exist, and scientific ethics review measures are in force.[31] But their focus is not individual rights; it is **state oversight and social stability.** AI firms must register algorithms with authorities, disclose technical details, and ensure outputs align with "core socialist values."[32] Citizens have little space to challenge surveillance or profiling. For India, the lesson is twofold: centralised control allows rapid deployment of AI at scale, but it also demonstrates the dangers of unchecked state power in eroding privacy and civil liberties.

United Kingdom: Adaptive Regulation.

The UK has opted for a "pro-innovation" approach, seeking to balance competitiveness with caution. Rather than one central AI law, it empowers sector regulators (like the health or finance regulators) to oversee AI applications in their domains, guided by cross-cutting principles of safety, accountability, and fairness.[33] A proposed central function will coordinate risks and ensure consistency. This model is deliberately flexible, designed to evolve with the technology. Its risk is uneven enforcement—but its advantage is agility, a feature India may find useful as it experiments with sector-specific AI policies.

Other Emerging Models.

Other jurisdictions are also shaping the global conversation. **South Africa** uses its Protection of Personal Information Act (POPIA) alongside an AI research centre to guide development. **Australia** has issued voluntary AI ethics guidelines, relying on self-regulation more than law.[34]

[31] Cyberspace Administration of China, *Interim Measures for the Management of Generative Artificial Intelligence Services* (2023).
[32] Id. arts. 5–7.
[33] U.K. Dep't for Science, Innovation & Tech., A Pro-Innovation Approach to AI Regulation (White Paper, 2023).
[34] Australian Government, *AI Ethics Principles* (2019); South African Centre for Artificial Intelligence Research, *Overview* (2022).

While these models are less comprehensive, they show how middle-income democracies are approaching AI cautiously, often emphasising capacity-building before binding regulation.

Lessons for India.

What do these models teach us? The EU shows the importance of embedding rights at the core. The U.S. highlights innovation but also the costs of fragmentation. China illustrates the perils of state-centric AI control, while the UK demonstrates the value of adaptability. India, with its constitutional commitment to dignity and equality, cannot blindly copy any one model. It must carve out its own path—one that combines the EU's rights-first philosophy with the UK's regulatory agility, while avoiding the pitfalls of U.S. inconsistency and Chinese overreach.

6. CONSTITUTIONAL CHALLENGES POSED BY AI

AI does not just raise abstract questions about technology—it collides directly with India's constitutional values. The risks are not futuristic; they are here and now. From biometric surveillance at protests to opaque algorithms deciding access to loans, AI touches the core of Articles 14, 19, and 21. The challenge lies in ensuring that the same Constitution that once confronted wiretaps and domiciliary visits is ready to confront facial recognition and algorithmic profiling.

Consent Without Choice.

At the heart of privacy is consent, yet AI often undermines it. Think of mobile apps that collect data silently in the background, or welfare schemes where participation is contingent on Aadhaar-based authentication. Here, "consent" becomes a fiction—users are left with little real choice. The result is a hollowing out of the principle that data should only be processed with meaningful, informed agreement.[35]

Opacity and the Right to Explanation.

Many AI systems operate as "black boxes." A student denied admission by an AI-driven evaluation system, or a job applicant rejected by an automated résumé screener, may never know why the decision was made. This lack of transparency conflicts with the right to

[35] Usha Ramanathan, *Aadhaar: From Welfare to Surveillance*, 9 Indian J. Const. L. 1, 12–14 (2015).

informational self-determination and makes effective judicial review nearly impossible. Scholars have argued that in the digital era, Article 21 must be read to include a **right to explanation** when decisions significantly affect individual rights.[36]

Discrimination and Algorithmic Bias.

AI systems are only as unbiased as the data fed into them. In India, where caste, gender, and religion already shape opportunities, algorithmic decision-making can reinforce structural inequalities. For instance, predictive policing tools trained on biased crime data may disproportionately target minority communities. Such outcomes clash with the constitutional promise of equality before the law under Article 14.[37]

Chilling Effect on Free Speech and Association.

Surveillance technologies like facial recognition and social media monitoring do not merely record behaviour—they alter it. Citizens aware of constant surveillance may hesitate to attend protests, join unions, or express dissent online. This "chilling effect" directly implicates Article 19(1)(a) (freedom of speech) and Article 19(1)(c) (freedom of association). Courts have long recognised that fundamental rights lose meaning if citizens self-censor under the shadow of surveillance.[38]

The Proportionality Test.

The Supreme Court in *Puttaswamy* established proportionality as the touchstone for testing privacy restrictions: (i) a legitimate aim, (ii) necessity, (iii) least intrusive means, and (iv) balancing of rights.[39] AI deployments by the State often fail this test. Blanket use of facial recognition in public spaces, without statutory safeguards or oversight, is neither the least intrusive method nor proportionate to the aim of public safety. This raises the possibility that constitutional courts will increasingly be called upon to review AI through the lens of proportionality.

[36] Shreya Rao, *The Right to Explanation in Indian Constitutional Law*, 13 NUJS L. Rev. 45, 49–52 (2020).
[37] Rashmi Dyal-Chand, *Algorithmic Bias and the Indian Constitution: The Challenge of Article 14*, 6 Indian L. & Tech. Rev. 77, 82–87 (2022).
[38] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶ 180.
[39] Id. at ¶ 325 (Chandrachud, J.) (articulating the proportionality test).

The Access-to-Justice Gap.

Finally, even when rights are violated, enforcing them is difficult. Filing writ petitions under Articles 32 or 226 requires resources and legal awareness that many citizens simply do not have. For marginalised communities, the cost of contesting algorithmic injustice is prohibitive. This creates a paradox: those most likely to be harmed by AI systems are often the least able to seek constitutional remedies.

Taken together, these challenges show that AI does not just create technical dilemmas—it raises constitutional crises. Privacy, equality, and freedom of expression are not theoretical values; they are lived rights that AI can erode in subtle but profound ways. Unless courts, legislators, and regulators adapt quickly, AI risks becoming the twenty-first century's most efficient tool of rights erosion.

7. CONSTITUTIONAL AND LEGAL REFORMS

If privacy is to survive in the age of Artificial Intelligence, India's constitutional framework must evolve. Declaring privacy a fundamental right in *Puttaswamy* was historic, but it was only the beginning. The real challenge lies in translating doctrine into enforceable safeguards that can withstand the speed and scale of AI.

An AI Rights Charter.

India urgently needs a legislative framework that articulates specific rights for citizens in relation to AI. This could include: (i) the right to explanation when decisions are made by algorithms; (ii) the right to correct or contest automated decisions; (iii) the right to opt out of profiling; and (iv) the right to human oversight in high-stakes areas like healthcare, policing, or credit.[40] Without such explicit recognition, the promises of Article 21 risk being hollow when confronted with the opacity of machine learning systems.

Strengthening Judicial Doctrine.

Courts have already developed tools to scrutinise privacy violations—the proportionality test

[40] Vrinda Bhandari & Renuka Sane, Towards a Rights-Respecting Data Protection Law in India, NIPFP Working Paper No. 408 (2021).

from *Puttaswamy* being the most notable.[41] But constitutional doctrine must now go further. Courts could interpret Articles 14 and 21 to impose a duty of **algorithmic fairness and transparency** on the State. Just as unreasonable restrictions on free speech are struck down, AI systems that disproportionately harm marginalised communities should be tested against constitutional equality standards. Judicial creativity will be essential in filling the gap until legislation matures.

An Independent AI Ethics Commission.

Law alone cannot keep up with the pace of technological change. India should establish an independent **AI Ethics Commission**, modelled loosely on regulatory watchdogs like the Election Commission or the Comptroller and Auditor General. Such a body could conduct algorithmic audits, issue binding ethical guidelines, and advise courts and legislatures on emerging risks.[42] Crucially, its independence from the executive would allow it to scrutinise government-led AI projects, which are often the most intrusive.

Embedding Privacy by Design.

Reform cannot be limited to legal doctrines—it must also be built into technology itself. The Constitution's spirit can be operationalised through **privacy by design**, where systems are architected to minimise data collection, anonymise sensitive information, and default to protective settings.[43] Embedding these principles at the design stage reduces the burden on courts and regulators downstream.

Constitutional Amendments? Not Yet.

Some scholars have argued that India may eventually need a constitutional amendment explicitly codifying the right to privacy as a standalone fundamental right, much like the right to education was added under Article 21A.[44] While this is an attractive idea, the immediate priority is less about rewriting the Constitution and more about enforcing existing guarantees through legislation, judicial interpretation, and independent oversight.

[41] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶ 325.
[42] Shalini Randeria, *Independent Regulators in the Age of Technology: Lessons for India*, 12 Indian J. Const. L. 55, 61–64 (2020).
[43] OECD, *Privacy by Design and by Default in AI Systems* (2019).
[44] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* 212–15 (2019).

Ultimately, reforms must recognise a simple truth: the Constitution is only as strong as the institutions that enforce it. Without proactive courts, independent regulators, and a vigilant civil society, privacy will remain a paper promise in the face of powerful AI technologies. The time to act is now—before AI systems become so deeply entrenched in governance that rolling them back becomes impossible.

8. POLICY AND PRACTICAL SOLUTIONS

Constitutional reforms alone cannot safeguard privacy; they need to be backed by practical measures that shape how AI is designed, deployed, and monitored. India has to think beyond abstract rights and focus on concrete tools that ordinary citizens can rely on.

Stronger Data Protection in Practice.

The **Digital Personal Data Protection Act, 2023** is a start, but its real test will be in implementation. Regulators must ensure that its core principles—purpose limitation, informed consent, data minimisation—are not reduced to bureaucratic box-ticking.[45] Enforcement must target both corporations and government agencies, especially in high-risk deployments like welfare schemes and policing. Without strict oversight, exemptions in the law will swallow the rule.

Privacy by Design and Default.

Technology can itself be part of the solution. AI systems should be built around privacy-protective features from the outset. This includes **anonymisation, pseudonymisation, minimal data retention**, and security safeguards as the default setting rather than an optional add-on.[46] International experience shows that embedding privacy at the design stage prevents downstream abuse and reduces the burden on regulators and courts.

Privacy-Enhancing Technologies (PETs).

Emerging tools like **differential privacy, federated learning, and homomorphic encryption** allow data to be used for training AI without exposing raw personal information.[47] For example,

[45] Digital Personal Data Protection Act, No. 22 of 2023 (India), §§ 5–9.
[46] OECD, *Privacy by Design and by Default in AI Systems* (2019).
[47] Cynthia Dwork & Aaron Roth, *The Algorithmic Foundations of Differential Privacy* (2014); Peter Kairouz et al., *Advances and Open Problems in Federated Learning*, 34 Found. & Trends Mach. Learn. 1 (2021).

federated learning lets algorithms learn from distributed datasets (like medical records) without moving the data out of hospitals. By mandating or incentivising PETs, India can harness AI's potential while reducing exposure of sensitive personal data.

Algorithmic Transparency and Impact Assessments.

Opaque decision-making is one of the biggest threats AI poses to privacy and dignity. Companies and government bodies deploying AI should be required to conduct **Data Protection Impact Assessments (DPIAs)** for high-risk systems.[48] These assessments can evaluate bias, fairness, and proportionality before deployment. Just as environmental clearances are mandatory before building a factory, algorithmic clearances should be mandatory before rolling out AI in sensitive areas.

Independent Oversight.

The Data Protection Board of India must not be the only watchdog. Sector-specific regulators—like those in finance, healthcare, or education—should be empowered to audit AI deployments in their fields. An independent AI oversight authority could also coordinate across sectors, conduct algorithmic audits, and publish transparency reports.[49] The credibility of any legal framework will depend on whether these bodies are independent and technically equipped.

Judicial Safeguards.

Courts, too, must adapt. The proportionality test laid down in *Puttaswamy* offers a ready-made tool for judicial review of AI systems: is the State's aim legitimate, is the intrusion necessary, is it the least intrusive means, and does the benefit outweigh the rights cost?[50] Applying this test to AI-driven surveillance or profiling will ensure constitutional rights remain central in the digital era.

Public Awareness and Digital Literacy.

Finally, privacy cannot be protected by law and technology alone. Citizens must know their rights and how to exercise them. Public awareness campaigns, digital literacy programs, and

[48] EU General Data Protection Regulation, art. 35 (requiring Data Protection Impact Assessments).
[49] Shalini Randeria, *Independent Regulators in the Age of Technology: Lessons for India*, 12 Indian J. Const. L. 55, 61–64 (2020).
[50] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶ 325.

civil society advocacy are critical. After all, a right unexercised is often a right lost. Empowering individuals to demand explanations, file grievances, and hold institutions accountable will create bottom-up pressure for compliance.

Taken together, these solutions form a multi-layered response: **law, technology, institutions, and civic participation.** Only when all four work in tandem can India strike the delicate balance between technological progress and constitutional protection.

9. CONCLUSION

Artificial Intelligence is no longer just a tool of the future—it is woven into the fabric of India's present. From Aadhaar-based welfare delivery to AI-powered surveillance cameras in smart cities, algorithms are already making decisions that affect our liberty, dignity, and equality. The question is not whether India will embrace AI, but on what terms.

The constitutional recognition of privacy in *Puttaswamy* was a watershed moment, but it was only the beginning. The challenge now is to carry that promise forward into an era where personal data is the fuel of governance and commerce. If left unchecked, AI could normalise mass surveillance, deepen social discrimination, and chill free expression. But with the right legal and institutional safeguards, it could also drive inclusive growth and empower citizens.

The path forward requires three commitments. First, a **rights-first approach**, where constitutional values guide the design and deployment of AI, not the other way around. Second, a **robust regulatory ecosystem**, one that combines strong data protection laws with algorithmic accountability, independent oversight, and sector-specific safeguards. And third, **citizen empowerment**, through awareness, literacy, and access to remedies, so that the right to privacy is not confined to courtrooms but lived in everyday life.

India stands at a crossroads. One path leads to technological growth that undermines constitutional freedoms. The other leads to a model where innovation and rights reinforce each other, making India not just a hub for AI development, but also a global leader in ethical and democratic AI governance.

If the Constitution is to remain a "living document," it must rise to this challenge. The future of AI in India should not be measured only in economic gains or technological milestones, but

in how well it preserves the dignity, liberty, and equality of every citizen. Growth without rights is not progress. A truly digital India must also be a constitutional India.

REFERENCES

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
2. Ministry of Housing & Urban Affairs, Government of India, *Smart Cities Mission Statement and Guidelines* (2017).
3. Ananth Padmanabhan, *The Illusion of Consent in India's Data Protection Regime*, Centre for Policy Research (2023).
4. UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
5. NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll* (2018).
6. Vidushi Marda & Shivangi Narayan, *Facial Recognition Technology in India: A Threat to Privacy and Civil Liberties*, Internet Freedom Foundation (2020).
7. OECD, *Recommendation of the Council on Artificial Intelligence* (2019).
8. Apar Gupta, *Deepfakes and the Indian Legal System: Gaps and Challenges*, Internet Democracy Project (2023).
9. Digital Personal Data Protection Act, No. 22 of 2023, § 13 (India).
10. EU General Data Protection Regulation
11. California Consumer Privacy Act (CCPA)