The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

Privacy in the Age of Artificial Intelligence and Digital Governance: Striking the Balance Between Innovation and Fundamental Rights

~ ROUBLE SRIVASTAVA

Introduction

Artificial Intelligence (AI) has rapidly transformed the way governments, businesses, and individuals interact with technology. From facial recognition systems and predictive policing to digital payment platforms and AI-powered healthcare, intelligent systems have become deeply integrated into modern governance. Governments across the world are increasingly relying on AI to improve public administration, enhance efficiency, and deliver citizen-centric services. While these developments promise faster decision-making and improved governance, they also raise serious concerns regarding privacy, data protection, and individual autonomy.

In the twenty-first century, data has emerged as one of the most valuable resources. Every online transaction, social media interaction, biometric authentication, GPS location, and internet search contributes to an individual's digital footprint. AI systems depend on massive datasets to function effectively, making the collection, processing, and analysis of personal information an essential part of their operation. However, this extensive use of personal data has blurred the line between technological convenience and intrusive surveillance. As AI becomes more sophisticated, the ability to predict human behaviour, influence decision-making, and monitor citizens has expanded significantly, making privacy one of the defining legal and ethical challenges of our time.

The debate surrounding privacy in the age of AI is not merely about protecting personal information; it concerns the preservation of human dignity, autonomy, and democratic values. Privacy enables individuals to exercise freedom of thought, expression, and association without unwarranted interference. When AI systems collect and process personal data without adequate safeguards, they risk creating an environment where individuals are constantly monitored, profiled, and evaluated through automated decision-making. Such practices may result in discrimination, exclusion, and violations of fundamental rights, particularly when algorithms operate without transparency or accountability.

In India, the significance of privacy gained constitutional recognition through the landmark judgment of ***Justice K.S. Puttaswamy (Retd.) v. Union of India***[1], wherein the Supreme Court unanimously declared the right to privacy as an intrinsic part of the right to life and personal liberty guaranteed under Article 21[2] of the Constitution. The judgment acknowledged that informational privacy is indispensable in the digital age and emphasized the State's obligation to establish adequate safeguards against arbitrary data collection and misuse. The subsequent enactment of the Digital Personal Data Protection Act, 2023[3] marked an important legislative step towards regulating personal data processing, although debates continue regarding the adequacy of its safeguards, exemptions, and enforcement mechanisms.

Globally, governments have adopted varying approaches to AI regulation. The European Union has attempted to establish a comprehensive framework through its risk-based regulatory model, while countries such as the United States, China, and the United Kingdom continue to develop sector-specific or policy-oriented approaches. These differing models demonstrate that AI governance is not solely a technological issue but also a constitutional, legal, and policy challenge that requires balancing innovation with the protection of fundamental rights.

In my opinion, privacy should not be viewed as an obstacle to technological advancement. Rather, it should function as the foundation upon which responsible innovation is built. AI undoubtedly offers unprecedented opportunities for economic growth, efficient governance, and improved public services. However, technological progress cannot come at the cost of constitutional freedoms. Digital governance must therefore evolve in a manner that promotes innovation while ensuring transparency, accountability, fairness, and respect for individual rights.

This article critically examines the relationship between artificial intelligence, privacy, and digital governance. It analyses the constitutional framework governing privacy, explores the challenges posed by AI-driven decision-making, evaluates India's emerging regulatory landscape in comparison with international developments, and argues that effective AI governance must place human rights at the centre of technological progress. Only by striking an appropriate balance between innovation and privacy can democratic societies fully realise the benefits of artificial intelligence without compromising the freedoms they seek to protect.

Understanding Artificial Intelligence, Digital Governance and the Concept of Privacy

Before examining the legal implications of AI, it is important to understand the relationship between artificial intelligence, digital governance, and privacy. These three concepts are closely interconnected and together define the nature of governance in the digital era. AI

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[2] INDIA CONST. art. 21.
[3] Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Extra., Part II, sec. 1 (Aug. 11, 2023).

serves as the technological engine, digital governance provides the institutional framework for its application, and privacy functions as the legal and ethical boundary that prevents the misuse of technology. A discussion on one cannot be complete without examining the other two.

Artificial Intelligence refers to the capability of computer systems to perform tasks that ordinarily require human intelligence. These tasks include learning from data, recognizing patterns, understanding language, making predictions, solving problems, and, in some cases, taking autonomous decisions. Unlike traditional software that follows predetermined instructions, AI systems improve their performance through continuous analysis of data. Machine learning, deep learning, natural language processing, and computer vision have enabled AI to become increasingly sophisticated, making it an indispensable part of governance and commercial activities[4].

Governments across the world have embraced AI as a tool for improving public administration. In India, digital governance has expanded significantly through initiatives such as Aadhaar-enabled service delivery, the Digital India Mission, DigiLocker, the Unified Payments Interface (UPI), e-Courts, CoWIN, and various AI-enabled public services. These initiatives have undoubtedly improved accessibility, reduced administrative delays, and enhanced transparency. Citizens today can access government services without visiting public offices, demonstrating how technology has transformed governance from a paper-based system into a digitally integrated ecosystem.

However, digital governance extends beyond digitising public services. It involves the collection, storage, sharing, and analysis of enormous volumes of personal data. Governments increasingly rely on data-driven decision-making to formulate policies, identify beneficiaries of welfare schemes, prevent fraud, and strengthen national security. AI enhances this process by enabling predictive analysis and automated decision-making. While these capabilities improve efficiency, they also expand the State's ability to monitor individuals, creating concerns regarding excessive surveillance and misuse of personal information.

Privacy, therefore, assumes a central role in AI-driven governance. Traditionally, privacy was understood as the right to be left alone. In the digital age, however, the concept has evolved considerably. Privacy now encompasses informational privacy, decisional autonomy, bodily integrity, and control over one's personal data. It enables individuals to determine how their information is collected, processed, shared, and retained. This understanding is particularly important because modern AI systems rely not merely on information voluntarily provided by individuals but also on behavioural data generated through routine digital activities.

One of the distinguishing characteristics of AI is its ability to infer information that individuals may never have explicitly disclosed. For example, a person's browsing history, purchase patterns, search queries, or social media activity may allow AI systems to predict

---

[4] Organisation for Economic Co-operation and Development (OECD), *OECD Principles on Artificial Intelligence* (2019), https://oecd.ai/en/ai-principles.

political opinions, religious beliefs, health conditions, financial status, or psychological characteristics. Such predictive capabilities create a new dimension of privacy concerns because individuals may lose control not only over the data they provide but also over the conclusions drawn from that data.

The concentration of personal data among governments and private technology companies has also altered the balance of power between individuals and institutions. Large digital platforms collect vast quantities of information regarding user behaviour, often using sophisticated AI systems to personalise content, target advertisements, and influence consumer choices. While these practices contribute to economic growth and innovation, they also create risks of manipulation, profiling, and behavioural control. Individuals frequently consent to data collection without fully understanding the extent to which their information may be processed or shared, raising concerns regarding the meaningfulness of digital consent.

These developments demonstrate that privacy can no longer be viewed solely as an individual concern. It has become a matter of public interest and democratic governance. A society in which individuals constantly fear surveillance or profiling may experience a chilling effect on free speech, association, and political participation. Thus, protecting privacy is not merely about safeguarding personal information; it is about preserving the conditions necessary for the exercise of constitutional freedoms.

Accordingly, understanding AI, digital governance, and privacy as interconnected concepts provides the foundation for analysing the constitutional framework governing informational privacy and the legal obligations of the State in an increasingly data-driven society.

The Constitutional Foundation of Privacy in India

The recognition of privacy as a constitutional right represents one of the most significant developments in Indian constitutional jurisprudence. Although the Constitution of India does not expressly mention the word "privacy," judicial interpretation has transformed it into an indispensable component of the right to life and personal liberty under Article 21[5]. This evolution reflects the judiciary's acknowledgment that constitutional rights must adapt to changing social and technological realities. In an era where artificial intelligence relies heavily on personal data, constitutional protection of privacy has become more relevant than ever.

The journey towards recognising privacy as a fundamental right was gradual. Early judicial decisions adopted a restrictive interpretation of personal liberty. In *M.P. Sharma v. Satish Chandra* (1954)[6], the Supreme Court held that the Constitution did not expressly recognise a right to privacy. Similarly, in *Kharak Singh v. State of Uttar Pradesh (1962)*[7], the majority declined to acknowledge privacy as an independent constitutional right, although it

[5] INDIA CONST. art. 21.
[6] *M.P. Sharma v. Satish Chandra*, A.I.R. 1954 S.C. 300 (India).
[7] *Kharak Singh v. State of Uttar Pradesh*, A.I.R. 1963 S.C. 1295 (India).

invalidated certain forms of police surveillance on the ground that they violated personal liberty. Justice Subba Rao's celebrated dissent, however, argued that privacy was inherent in the concept of ordered liberty and deserved constitutional protection. This dissent later became the foundation for subsequent judicial developments.

Over time, the Supreme Court gradually expanded the scope of Article 21 through a purposive interpretation. Decisions such as *Gobind v. State of Madhya Pradesh* (1975)[8], *R. Rajagopal v. State of Tamil Nadu* (1994)[9], and *People's Union for Civil Liberties (PUCL) v. Union of India* (1997)[10] progressively recognised various dimensions of privacy, including protection against unlawful surveillance and unauthorised disclosure of personal information. These decisions indicated that privacy was closely linked with dignity, autonomy, and individual freedom, even though its precise constitutional status remained uncertain.

The uncertainty was conclusively resolved in *Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)*[11], where a nine-judge Constitution Bench unanimously declared that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution. The judgment overruled the contrary observations in *M.P. Sharma* and *Kharak Singh*, firmly establishing privacy as an essential element of constitutional liberty. The Court emphasised that privacy is intrinsic to human dignity, individual autonomy, and the free development of personality. Importantly, it recognised informational privacy as a distinct constitutional interest requiring protection in the digital age.

The significance of *Puttaswamy* extends far beyond its declaration of privacy as a fundamental right. The Court acknowledged that advances in technology had fundamentally altered the relationship between individuals, the State, and private corporations. It observed that digital technologies enable the collection, storage, and processing of enormous quantities of personal information, creating unprecedented opportunities for surveillance and profiling. Consequently, the Court stressed that any restriction upon privacy must satisfy the constitutional requirements of legality, legitimate state purpose, necessity, and proportionality.

The proportionality principle established in *Puttaswamy* has become the constitutional benchmark for evaluating State action involving personal data. First, there must exist a valid law authorising the interference. Secondly, the law must pursue a legitimate governmental objective. Thirdly, the measure adopted must be necessary to achieve that objective. Finally, the restriction must be proportionate, ensuring that the least intrusive means are employed. These safeguards are particularly relevant in assessing AI-enabled surveillance systems, facial recognition technologies, predictive policing mechanisms, and large-scale data analytics undertaken by public authorities.

---

[8] *Gobind v. State of Madhya Pradesh*, (1975) 2 S.C.C. 148 (India).
[9] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 S.C.C. 632 (India).
[10] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 S.C.C. 301 (India).

[11] Supra note 1

The constitutional framework also reflects an inherent balance between individual liberty and legitimate governmental interests. Privacy is not an absolute right. The State may impose reasonable restrictions for purposes such as national security, public order, crime prevention, or public health, provided such measures satisfy constitutional scrutiny. This balanced approach is especially significant in the context of AI governance, where technological innovation frequently intersects with security concerns and administrative efficiency.

From my perspective, the true contribution of *Puttaswamy* lies not merely in recognising privacy as a legal entitlement but in redefining the relationship between citizens and the digital State. The judgment affirms that constitutional values cannot be compromised merely because technological capabilities have advanced. AI may transform governance, but constitutional principles must continue to govern AI.

Digital Governance in India: Opportunities and Risks

India has emerged as one of the world's leading digital economies through initiatives such as Digital India, Aadhaar, DigiLocker, Unified Payments Interface (UPI), e-Courts, and the CoWIN vaccination platform. These initiatives have transformed public administration by making government services more accessible, transparent, and efficient. AI is increasingly being integrated into governance for fraud detection, traffic management, healthcare diagnostics, agricultural advisory services, and smart city projects. Such innovations demonstrate the immense potential of technology to improve governance and promote inclusive development[12].

Despite these achievements, digital governance also presents complex legal and ethical concerns. Most digital platforms rely on extensive data collection to function effectively. Citizens frequently provide personal information to access essential public services, often without fully understanding how their data will be processed, shared, or retained. The imbalance between the State's data-gathering capabilities and the individual's ability to control personal information raises concerns regarding informational self-determination.

Another significant challenge is the absence of complete transparency in algorithmic governance. Automated systems used for public decision-making may affect welfare distribution, law enforcement, taxation, or administrative investigations. If citizens are denied benefits or subjected to adverse decisions without understanding the basis of an algorithmic assessment, principles of natural justice and procedural fairness may be compromised. Accountability becomes particularly difficult when AI systems function as "black boxes," making it impossible to explain how a particular outcome was reached.

In my view, India's digital transformation is an undeniable success story, but technological progress must remain people-centric. Digital governance should enhance citizens' trust rather

[12] Digital India Programme (last visited Aug. 2, 2026).

than expand institutional power. Privacy, transparency, and accountability must therefore become foundational principles guiding every stage of digital policymaking and AI deployment.

The Digital Personal Data Protection Act, 2023 and India's Emerging AI Regulatory Framework

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act)[13] marked a significant milestone in India's journey towards establishing a comprehensive data protection regime. Enacted following the constitutional recognition of privacy in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[14], the legislation seeks to regulate the processing of digital personal data while balancing individual rights with legitimate governmental and commercial interests. It introduces obligations upon data fiduciaries, recognises the rights of data principals, and establishes mechanisms for consent-based processing, grievance redressal, and regulatory oversight.

The Act grants individuals important rights, including the right to access information regarding data processing, seek correction or erasure of personal data, nominate another person to exercise rights in certain circumstances, and approach the Data Protection Board in cases of non-compliance. These provisions reflect an effort to strengthen informational autonomy in an increasingly digital society. However, the legislation has also attracted criticism for providing broad exemptions to the State under specified circumstances. Critics argue that extensive governmental exemptions may dilute the constitutional safeguards recognised in *Puttaswamy*, particularly where surveillance or national security considerations are invoked.

At present, India does not possess a standalone statute exclusively regulating artificial intelligence. Instead, AI governance is developing through policy initiatives, sector-specific regulations, and ethical frameworks such as **NITI Aayog's Responsible AI for All**[15] approach. While these initiatives promote innovation, they remain largely non-binding and therefore provide limited legal certainty.

Challenges in Regulating AI: Ethical, Legal and Practical Issues

Despite its transformative potential, regulating artificial intelligence remains one of the greatest legal challenges of the digital age. AI systems evolve rapidly, whereas legislation often develops gradually. This mismatch creates regulatory gaps that allow emerging

[13] Supra note 3
[14] Supra note 1
[15] NITI Aayog, *Responsible AI for All: Approach Document for India Part I—Principles for Responsible AI* (2021).

technologies to operate without adequate legal oversight. Policymakers therefore face the difficult task of encouraging innovation while simultaneously protecting constitutional rights.

One significant challenge is the lack of transparency in AI decision-making. Many advanced AI systems operate through complex algorithms that even their developers struggle to interpret. This "black box"[16] phenomenon makes it difficult for individuals to understand why a particular decision was made or to challenge automated outcomes effectively. Such opacity conflicts with the principles of natural justice and administrative accountability.

Another concern is algorithmic discrimination. AI systems trained on biased or incomplete datasets may perpetuate historical inequalities by disproportionately affecting marginalised communities. Automated recruitment systems, predictive policing tools, or credit-scoring algorithms may unintentionally discriminate on the basis of caste, gender, religion, or socio-economic background. Without regular audits and human oversight, AI risks reinforcing existing social prejudices rather than eliminating them.

Cross-border data flows further complicate AI governance. Personal information often travels across multiple jurisdictions, making enforcement of domestic privacy laws increasingly difficult. Questions relating to jurisdiction, liability, and regulatory cooperation remain largely unresolved.

In my opinion, AI governance should adopt a human-centric approach. Technology must remain accountable to constitutional values rather than replacing them. Effective regulation should therefore prioritise transparency, explainability, fairness, periodic algorithmic audits, and meaningful human intervention in decisions that significantly affect individual rights.

Recommendations and the Way Forward

As artificial intelligence becomes an integral component of governance, India must adopt a comprehensive regulatory strategy that balances innovation with constitutional safeguards. The existing legal framework provides an important starting point, but a dedicated AI governance mechanism is necessary to address the unique challenges posed by automated decision-making and large-scale data processing.

First, India should enact a **comprehensive AI legislation** incorporating principles of transparency, explainability, accountability, and human oversight. High-risk AI systems deployed in sectors such as law enforcement, healthcare, finance, and public administration should undergo mandatory risk assessments and independent algorithmic audits before implementation.

Secondly, privacy should be embedded into technological design through the principle of **privacy by design**. AI developers and public authorities should collect only the minimum amount of personal data necessary for a legitimate purpose while ensuring strong

[16] Frank Pasquale, *The Black Box Society* (Harvard Univ. Press 2015).

cybersecurity safeguards. Citizens must also receive clear and accessible information regarding how their data is processed and how automated decisions affect them.

Thirdly, an **independent AI regulatory authority** should be established to monitor compliance, investigate complaints, and issue sector-specific guidelines. Collaboration between government agencies, academia, industry, and civil society would further strengthen responsible AI governance.

Finally, digital literacy should become a national priority. Citizens who understand their privacy rights are better equipped to make informed decisions regarding data sharing and online participation.

In my opinion, India should not view privacy and innovation as competing objectives. Instead, they should function as complementary values. Responsible AI governance can foster technological advancement while simultaneously strengthening public trust, democratic accountability, and constitutional governance.

Conclusion

Artificial intelligence has fundamentally transformed the relationship between individuals, technology, and the State. Its integration into governance has improved administrative efficiency, expanded access to public services, and accelerated digital innovation. At the same time, AI has introduced unprecedented challenges relating to privacy, surveillance, algorithmic discrimination, and accountability. These concerns demonstrate that technological progress cannot be evaluated solely in terms of efficiency; it must also be measured by its impact on fundamental rights and democratic values.

India has taken significant steps towards protecting informational privacy through the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* and the enactment of the Digital Personal Data Protection Act, 2023. However, the rapidly evolving nature of AI demands a more comprehensive and forward-looking regulatory framework. Future governance should be guided by constitutional principles of legality, proportionality, transparency, fairness, and human dignity while ensuring that innovation continues to flourish.

In my view, the future of digital governance should not be characterised by a choice between privacy and technological development. The true challenge lies in creating systems that advance both simultaneously. AI should remain a tool that empowers citizens rather than monitors them, enhances governance rather than diminishes accountability, and strengthens democracy rather than weakening individual freedoms. Only by placing human rights at the centre of AI regulation can India build a digital future that is both innovative and constitutionally resilient