JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

"AI AND THE RIGHT TO PRIVACY: ANALYSING THE SCOPE OF INFORMATIONAL AUTONOMY UNDER ARTICLE 21"

[1]SANJANA AGGARWAL
[1]ASSISTANT PROFESSOR
[1]GEETA INSTITUE OF LAW, PANIPAT

Abstract

The rapid proliferation of Artificial Intelligence (AI) technologies in governance, commerce, and surveillance has posed significant challenges to the individual's right to privacy under Article 21 of the Indian Constitution. In particular, the notion of informational autonomy—the right of individuals to control the collection, use, and dissemination of their personal data— has emerged as a critical dimension of privacy in the digital era. This paper explores the intersection of AI and privacy law, focusing on how automated decision-making, profiling, and mass data surveillance impact the constitutional guarantee of privacy as interpreted by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*[1]. While the Court affirmed privacy as a fundamental right, the evolving nature of AI tools challenges the enforcement of this right, particularly when consent becomes illusory or opaque.

This study analyzes India's current legal landscape, including the Digital Personal Data Protection Act, 2023[2], and compares it with international standards such as the EU General Data Protection Regulation (GDPR)[3]. The paper argues that while India has made strides in recognising digital rights, the regulatory framework remains inadequate to address the risks posed by AI to informational autonomy. Drawing from jurisprudence, international best practices, and ethical AI principles, the paper proposes a rights-centric approach to AI governance that balances innovation with individual freedoms. The study concludes with policy recommendations to strengthen safeguards for informational autonomy in AI-driven environments, ensuring that the promises of digital progress do not come at the cost of constitutional liberties[4,5].

---

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

[2] Digital Personal Data Protection Act, 2023 (India).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), *Official Journal of the European Union*, L 119/1, 2016.

[4] Sethi, A., "Privacy in the Age of Artificial Intelligence: Indian Legal Framework and Challenges", *NLIU Law Review*, Vol. XI, 2022, pp. 104-122.

[5] Bhandari, V., "Artificial Intelligence and Fundamental Rights: Rethinking Privacy in the Algorithmic Era", *NUJS Law Review*, Vol. 14, No. 2, 2021, pp. 1-25.

Keywords: *Artificial Intelligence (AI), Right to Privacy, Article 21, Informational Autonomy, Data Protection, Algorithmic Governance, Digital Personal Data Protection Act, 2023, Puttaswamy Judgment, Automated Decision-Making, Mass Surveillance, Datafication, Constitutional Rights, AI Ethics, Fundamental Rights in India, Consent and Privacy, Profiling and Discrimination, GDPR and Comparative Analysis, Privacy by Design, Predictive Technologies, Human Dignity and Technology.*

Introduction

The emergence of Artificial Intelligence (AI) has fundamentally transformed the digital landscape, influencing decisions in sectors ranging from healthcare and finance to law enforcement and social governance. These developments, while promising, raise significant concerns about the protection of individual rights, especially the right to privacy. AI systems rely heavily on vast datasets to function, often incorporating sensitive personal information without the knowledge or informed consent of individuals. This data-driven nature of AI has direct implications for informational autonomy—the right to control one's personal data— which is now considered a core component of the right to privacy in India.

In the landmark judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court unanimously declared that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution of India[6]. The Court not only recognized privacy as a standalone fundamental right but also emphasized its informational dimension, stating that individuals have a right to control the dissemination and use of their personal data. This aspect of privacy—informational autonomy—has become increasingly relevant in the age of AI where technologies can track, profile, and make decisions about individuals based on data analytics and predictive algorithms[7].

However, the constitutional recognition of privacy has not yet been matched with comprehensive legislative or regulatory frameworks capable of curbing AI's invasive potential. While the Digital Personal Data Protection Act, 2023 attempts to address these concerns, it has been criticized for being lenient on state surveillance and opaque algorithmic practices[8]. In contrast, international frameworks such as the EU's General Data Protection Regulation (GDPR) provide a more robust foundation for ensuring transparency, accountability, and individual control over data processing[9]. This paper explores these intersections—between constitutional rights, technological advances, and regulatory responses—to critically examine how well Indian law protects informational autonomy in the face of rapidly evolving AI technologies.

---

[6] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

[7] Bhandari, V., "Artificial Intelligence and Fundamental Rights: Rethinking Privacy in the Algorithmic Era", *NUJS Law Review*, Vol. 14, No. 2, 2021, pp. 1–25.

[8] Digital Personal Data Protection Act, 2023 (India)

"Constitutional Right to Privacy under Article 21" Evolution of the Right to Privacy in India

The recognition of the right to privacy in India has undergone a transformative constitutional journey. Initially, in *Kharak Singh* v. *State of U.P.*[10], the Supreme Court rejected the claim that privacy was a protected constitutional right, despite expressing concerns about domiciliary visits by the police. Similarly, in *MP Sharma* v. *Satish Chandra*[11], an eight-judge bench held that the Constitution did not explicitly guarantee a right to privacy. These early judgments reflected a narrow interpretation of personal liberty under Article 21.

The tide began to turn in subsequent rulings, especially in cases such as *Gobind v. State of Madhya Pradesh*[12], where the Court acknowledged that privacy could be protected under Article 21, albeit not as an absolute right. The landmark moment came with the unanimous nine-judge bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[13], which overturned the earlier precedents and categorically affirmed that the right to privacy is a fundamental right inherent in Article 21 and other freedoms guaranteed by Part III of the Constitution. The Court emphasized that privacy encompasses physical and bodily integrity, decisional autonomy, and informational self-determination.

Informational Autonomy as a Subset of Privacy

One of the most significant contributions of the *Puttaswamy* judgment was the acknowledgment of informational autonomy as a subset of privacy. Informational autonomy refers to the individual's right to control the collection, usage, and dissemination of their personal data. The Court noted that in the digital age, protecting privacy must necessarily

include protecting the informational choices that individuals make, especially when interacting with the state or private entities[14].

This interpretation aligns with global jurisprudence, including the European Court of Human Rights' recognition of the right to control personal data as part of the broader right to private life[15]. In the Indian context, this aspect becomes crucial as state-led initiatives like Aadhaar and data-driven governance models expand rapidly, often without adequate consent mechanisms. The Court underscored that informational privacy is critical to maintaining human dignity and must be safeguarded even as the state pursues technological innovations for public welfare.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), *Official Journal of the European Union*, L 119/1, 2016.
[10] *Kharak Singh* v. *State of U.P.*, AIR 1963 SC 1295
[11] *MP Sharma v. Satish Chandra*, AIR 1954 SC 300
[12] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Judicial Interpretation and Expansion of Article 21

The jurisprudence surrounding Article 21 has progressively expanded the meaning of "life and personal liberty" to include a wide range of substantive rights. From the right to shelter and education to reproductive autonomy and health, Article 21 has been interpreted as a living provision that adapts to changing times. The right to privacy is now firmly embedded within this framework, reaffirmed not only in *Puttaswamy* but also in *Anuradha Bhasin v. Union of India*[16], where the Court emphasized the importance of proportionality and necessity when restricting digital freedoms.

The evolution reflects a shift from a limited textual reading of the Constitution to a purposive interpretation that recognizes privacy as essential to human dignity. Judicial recognition of privacy as a foundational right not only strengthens civil liberties but also imposes a constitutional obligation on the state to protect citizens against intrusive technologies, including AI-based systems. This growing judicial emphasis on informational autonomy within the framework of Article 21 sets the stage for deeper scrutiny of data collection and processing practices in both public and private sectors.

"Understanding AI and Its Impact on Privacy" What is Artificial Intelligence?

Artificial Intelligence (AI) refers to computer systems or machines that perform tasks requiring human intelligence, such as learning, reasoning, decision-making, and pattern recognition. These systems are designed to simulate human cognitive functions and can be classified into narrow AI (task-specific) and general AI (multi-tasking systems). The development of AI technologies such as natural language processing, machine learning, and neural networks has enabled machines to interpret, analyze, and respond to data inputs in increasingly sophisticated ways (Bhandari, 2021)[17]. While AI offers benefits across domains—from healthcare diagnostics to financial forecasting—it also raises profound concerns about autonomy, discrimination, and privacy, especially when implemented without transparency or oversight.

[14] Ibid.
[15] Case of *S. and Marper v. United Kingdom*, Application Nos. 30562/04 and 30566/04, European Court of Human Rights (2008).
[16] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

Mechanisms of Data Collection and Processing by AI Systems

AI systems rely on massive amounts of data to function effectively. This data is collected through digital footprints left across devices, platforms, and services—ranging from biometric identifiers and location data to search histories and behavioural patterns. The processing involves algorithms that analyse, predict, and automate decisions based on data patterns, often without human intervention. Such models improve as more data is fed into them—a process known as

supervised or unsupervised machine learning.

However, this raises several privacy concerns. First, individuals may not be aware that their data is being collected, let alone how it is used. Second, AI systems often lack transparency— decisions are made in a "black box" manner, where even developers may not fully understand the logic behind outputs. Third, data once collected may be stored indefinitely or reused for unrelated purposes, violating principles of data minimization and purpose limitation (Sethi, 2022)[18]. Without strict data governance, these mechanisms threaten the principle of informational autonomy recognized in *Puttaswamy*[19].

Use Cases Impacting Privacy (e.g., Facial Recognition, Predictive Policing, Social Scoring)

Several real-world applications of AI in India and globally have raised red flags from a privacy standpoint. One prominent example is facial recognition technology (FRT), used by Indian law enforcement agencies without statutory regulation or citizen consent. The deployment of the Automated Facial Recognition System (AFRS) by police departments across India has been criticized for its potential to enable mass surveillance and chilling effects on public freedoms (Bhandari, 2021).

Predictive policing is another area where AI algorithms use historical crime data to forecast future offenses or identify suspects. While touted as efficient, such systems often perpetuate existing biases and disproportionately target marginalized communities. These algorithmic tools lack transparency and are rarely subject to independent audits or constitutional safeguards.

A third concern is social scoring systems, as seen in China, where citizens are ranked based on their online and offline behaviours. Although India does not currently operate a formal social credit system, similar practices can emerge through credit scoring apps, fintech platforms, or AI-driven behavioural analytics used by employers, insurers, and the government.

All these use cases reflect how AI can erode privacy by normalizing data-driven surveillance and automating decisions that significantly affect individual rights. Without meaningful legal checks, AI risks undermining the core of informational autonomy under Article 21.

---

[17] Bhandari, V., *"Artificial Intelligence and Fundamental Rights: Rethinking Privacy in the Algorithmic Era"*, NUJS Law Review, Vol. 14, No. 2, 2021, pp. 1–25.
[18] Sethi, A., *"Privacy in the Age of Artificial Intelligence: Indian Legal Framework and Challenges"*, NLIU Law Review, Vol. XI, 2022, pp. 104–122.
[19] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

"Informational Autonomy in the Age of AI"

Definition and Significance of Informational Autonomy

Informational autonomy refers to an individual's ability to control the collection, use, and dissemination of their personal data. It is rooted in the broader concept of personal autonomy and is essential to maintaining human dignity, self-determination, and liberty. In the landmark *Justice K.S. Puttaswamy (Retd.) v. Union of India* case, the Supreme Court of India explicitly recognized informational autonomy as a component of the right to privacy under Article 21 of the Constitution[20]. The judgment emphasized that an individual's right to make choices about their digital presence and personal information is not just a matter of policy but a constitutional imperative.

In the age of AI, where machines are capable of making decisions based on massive volumes of personal data, the scope and importance of informational autonomy become even more critical. Without the ability to control how one's data is used—especially by opaque, automated systems—the individual risks losing agency and becoming subject to technological determinism.

---

[20] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Datafication and the Loss of Consent

The term datafication describes the process by which human behaviours, choices, and interactions are translated into quantifiable data. Every action—from online shopping and social media usage to biometric scans and GPS movement—feeds into digital ecosystems that are mined and monetized. AI thrives on this constant stream of data, using it to refine algorithms and deliver personalized services.

However, this process often bypasses informed consent. While many platforms claim to obtain user permission through terms and conditions, such consent is frequently obtained through deceptive design or legal complexity that renders the user unaware of what they are agreeing to (Sethi, 2022)[21]. The illusion of control masks a significant erosion of autonomy, especially in cases where AI systems collect data passively or infer sensitive information indirectly.

This "loss of consent" is particularly problematic when AI systems are deployed by the state or in essential services like banking, healthcare, or law enforcement. Individuals may have no meaningful choice but to comply, even when their data is used beyond its original purpose. The Supreme Court in *Puttaswamy* warned that data collected for one purpose cannot be repurposed without fresh consent, reinforcing the link between purpose limitation and individual dignity.

Profiling, Surveillance, and Algorithmic Decision-Making

One of the most alarming threats to informational autonomy in the AI era is the ability of systems to profile individuals—automatically categorizing them based on behavioural patterns, demographics, or predictive indicators. This profiling can be used to offer targeted advertisements, deny access to credit, or flag individuals for scrutiny, often without their knowledge or recourse.

AI-powered surveillance tools, such as biometric monitoring, facial recognition, and predictive policing, increasingly blur the line between security and control. In the absence of judicial or legislative oversight, such systems risk turning democracies into surveillance states (Bhandari, 2021)[22]. Surveillance not only invades privacy but also has a chilling effect on free speech and dissent.Further complicating matters is algorithmic decision-making, where automated systems make or influence critical decisions affecting individuals—such as employment screening, loan approvals, or social benefit eligibility. These decisions, often derived from biased or incomplete datasets, are rarely explainable and almost never appealable. This lack of transparency violates core principles of fairness and due process.

The European Union's GDPR tries to counter this through provisions like the "right to explanation" and "right to object" to automated processing[23]. In contrast, Indian law is still evolving, and the recently enacted Digital Personal Data Protection Act, 2023, does not fully address the risks posed by AI-driven profiling and decision-making[24]. This regulatory gap puts informational autonomy—and constitutional privacy guarantees—at significant risk.

---

[21] Sethi, A., *"Privacy in the Age of Artificial Intelligence: Indian Legal Framework and Challenges"*, NLIU Law Review, Vol. XI, 2022, pp. 104–122.

Existing Laws on Data Protection and AI (e.g., IT Act, 2000; DPDP Act, 2023)

India's journey toward comprehensive data protection legislation began with the Information Technology Act, 2000, which includes provisions for cybersecurity, data breaches, and unauthorized access. Section 43A and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, impose limited obligations on body corporates for protecting personal data. However, these provisions are outdated and were never designed to address the complex challenges posed by Artificial Intelligence (AI), such as algorithmic profiling, predictive analytics, or mass surveillance.

Recognizing the limitations of the IT Act, the Indian Parliament enacted the Digital Personal Data Protection (DPDP) Act, 2023. The Act establishes a framework for lawful data processing based on consent, purpose limitation, and data minimization. It introduces the roles of "data fiduciaries" and "data principals" and provides for rights such as access to data

and grievance redressal mechanisms[25]. While the DPDP Act represents a significant advancement in acknowledging data rights, it does not directly address AI-specific risks, such as opacity in algorithmic decision-making or the need for explainability in AI systems (Sethi, 2022)[26].

Moreover, the Act provides wide exemptions for government agencies under Section 17, allowing the state to process personal data without consent in the name of national interest or public order. This raises constitutional concerns, especially when such exemptions are not narrowly tailored or subject to judicial oversight, potentially undermining the privacy protections recognized in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[27].

---

[22] Bhandari, V., *"Artificial Intelligence and Fundamental Rights: Rethinking Privacy in the Algorithmic Era"*, NUJS Law Review, Vol. 14, No. 2, 2021, pp. 1–25.
[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), *Official Journal of the European Union*, L 119/1, 2016.
[24] Digital Personal Data Protection Act, 2023 (India).
[25] Ibid.

Gaps in the Legal Framework

Despite the enactment of the DPDP Act, India's legal regime still falls short of addressing the unique threats posed by AI technologies. One of the major gaps is the lack of AI-specific regulation. There is no legal requirement for algorithmic transparency, fairness audits, or accountability mechanisms for AI systems. Additionally, terms such as "profiling," "automated decision-making," and "AI ethics" are conspicuously absent from the DPDP Act.

Furthermore, user consent mechanisms remain weak, with platforms often presenting take-it- or-leave-it choices that lack granularity or comprehension. The current legal regime does not ensure the right to explanation, data portability, or objection to automated profiling, leaving individuals vulnerable to decisions made by unaccountable algorithms (Bhandari, 2021)[28]. Enforcement too is a concern, as the DPDP Act centralizes regulatory authority in a government-appointed Data Protection Board, whose independence has been questioned.

These gaps are particularly alarming given the increasing use of AI in law enforcement, financial risk scoring, and welfare distribution—areas with direct implications for constitutional rights.

Comparative Analysis: EU GDPR vs. Indian Legal Regime

The European Union's General Data Protection Regulation (GDPR), enforced in 2018, remains a global benchmark for data protection legislation. The GDPR enshrines robust rights such as the right to be forgotten (Article 17), right to data portability (Article 20), and right to object to automated decision-making (Article 22). It also mandates privacy by design, explicit and informed consent, and transparency in data processing[29].

In comparison, India's DPDP Act lacks clarity on key issues like automated profiling, purpose limitation in AI contexts, and meaningful consent. While the GDPR places strict obligations on data controllers and processors, India's law provides government agencies with sweeping powers that are not adequately counterbalanced by independent oversight or effective remedies. For instance, the GDPR's independent supervisory authorities are empowered to conduct audits and impose penalties, whereas India's Data Protection Board has limited powers and lacks structural autonomy.

Another area where the GDPR excels is in algorithmic accountability. Under Article 22, data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which significantly affects them. Indian law, on the other hand, does not offer such procedural safeguards, placing individuals at a significant disadvantage in an AI-governed ecosystem (Sethi, 2022).

Thus, while the DPDP Act represents progress, India must adopt a more comprehensive, AI- aware data protection framework that aligns with global best practices and upholds the constitutional mandate of informational autonomy.

[26] Sethi, A., *"Privacy in the Age of Artificial Intelligence: Indian Legal Framework and Challenges"*, NLIU Law Review, Vol. XI, 2022, pp. 104–122.
[27] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[28] Bhandari, V., *"Artificial Intelligence and Fundamental Rights: Rethinking Privacy in the Algorithmic Era"*, NUJS Law Review, Vol. 14, No. 2, 2021, pp. 1–25.

Challenges in Ensuring Privacy in AI Systems

Artificial Intelligence (AI) systems are reshaping governance, commerce, and daily life, but their increasing reliance on vast amounts of personal data has generated new challenges for safeguarding privacy. While the constitutional right to privacy is now firmly entrenched under Article 21, the ability to enforce this right effectively in the AI context remains uncertain. This section identifies and explores the principal obstacles to privacy protection in AI-driven environments.

Lack of Transparency and Explainability

A fundamental challenge lies in the opacity of AI algorithms, often referred to as the "black box" problem. Many AI systems, especially those based on deep learning, operate in ways that are not interpretable even by their developers. This lack of explainability undermines the ability of users to understand how decisions are made and precludes meaningful oversight. For example, an AI system used for credit scoring may deny a loan based on patterns in data that the individual cannot contest or comprehend (Bhandari, 2021)[30].

From a legal standpoint, the right to know how decisions are made is essential to the principle of natural justice and procedural fairness. The absence of algorithmic transparency violates the individual's informational autonomy and weakens accountability mechanisms. This issue is particularly critical in state-administered AI systems, where decisions can have life-altering consequences but lack statutory safeguards.

[29] Regulation (EU) 2016/679 (General Data Protection Regulation), *Official Journal of the European Union*, L 119/1, 2016.

Consent Mechanism and Informed Choice

Traditional notions of consent are ill-suited for AI systems. Consent today is often reduced to a formality—users are presented with complex privacy policies, which they accept without reading or understanding. In many AI applications, especially those involving biometric or behavioural data, consent is passively obtained or bypassed entirely through surveillance technologies.

The Digital Personal Data Protection Act, 2023 mandates consent as the legal basis for processing personal data, but it does not provide for granular consent specific to AI uses[31]. Nor does it address secondary data uses where data collected for one purpose is repurposed by AI for entirely different objectives. This is contrary to the *Puttaswamy* judgment, where the Court emphasized that consent must be informed, specific, and revocable[32].

In practice, the power imbalance between data fiduciaries and individuals further complicates consent. Users of public services or low-cost platforms may feel compelled to share data due to lack of alternatives, rendering consent coercive rather than voluntary.

Risk of Data Misuse and Unauthorized Surveillance

AI systems enable large-scale surveillance through data aggregation, facial recognition, and real-time tracking. In the absence of comprehensive surveillance laws in India, such technologies have been adopted without clear oversight or legal thresholds. Projects like Aadhaar, automated facial recognition by police, and predictive policing tools have raised

alarm among privacy advocates and scholars (Sethi, 2022)[33].

While public safety and governance efficiency are often cited as justifications, these deployments create an environment of pervasive surveillance, infringing on the right to privacy and the freedom to dissent. The Supreme Court in Anuradha Bhasin v. Union of India underscored that any restriction on fundamental rights must satisfy the tests of legality, necessity, and proportionality[34]. Yet, in AI-enabled surveillance practices, these standards are frequently ignored.

Additionally, private actors also use AI tools to profile users, predict behaviour, and influence choices—such as in targeted advertising and algorithmic news feeds. Without strong data protection enforcement or AI regulation, there is little deterrent to the misuse of personal data in ways that undermine individual autonomy.

[30] Bhandari, V., *"Artificial Intelligence and Fundamental Rights: Rethinking Privacy in the Algorithmic Era"*, NUJS Law Review, Vol. 14, No. 2, 2021, pp. 1–25.

[31] Digital Personal Data Protection Act, 2023 (India).

[32] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Judicial and Policy Responses to AI-Induced Privacy Concerns

The judiciary in India has played a pivotal role in shaping the contours of the right to privacy, especially in response to technological threats. However, while courts have recognized informational autonomy and digital rights, specific jurisprudence on Artificial Intelligence (AI) remains limited. At the same time, policy frameworks and committee reports have begun to acknowledge the urgent need for AI regulation. This section highlights both judicial precedents and policy efforts that attempt to address AI-induced privacy risks.

Role of the Indian Judiciary in Shaping Digital Privacy Norms

The landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[35] laid the foundation for a robust constitutional right to privacy under Article 21, affirming that privacy is not merely a negative right but a facet of dignity, autonomy, and personhood. The Supreme Court explicitly recognized informational privacy and stated that individuals have the right to control the dissemination of personal data.

Subsequently, in *Anuradha Bhasin v. Union of India*, the Court emphasized the proportionality test in state-imposed restrictions on digital rights, asserting that access to the internet is integral to freedom of expression[36]. While these decisions signal judicial sensitivity to technological overreach, courts have yet to develop a consistent doctrine concerning AI-specific threats like algorithmic discrimination, lack of explainability, or surveillance-based profiling.

In *Internet and Mobile Association of India v. RBI*[37], the Supreme Court struck down a blanket ban on cryptocurrency trading, observing that the restriction lacked proportional justification. Though unrelated to AI, the judgment reflects judicial willingness to scrutinize tech-related restrictions under constitutional standards. As AI becomes increasingly embedded in state and private systems, the judiciary may be called upon to develop new principles to assess algorithmic harm.

However, in the absence of detailed AI-related legislation, courts have struggled to offer concrete remedies in cases involving data breaches, facial recognition, or digital profiling. The lack of precedent leaves ambiguity around legal accountability and due process in algorithmic governance.

[33] Sethi, A., *"Privacy in the Age of Artificial Intelligence: Indian Legal Framework and Challenges"*, NLIU Law Review, Vol. XI, 2022, pp. 104–122.

[34] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

[35] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Policy Initiatives and Expert Committees on AI Governance

The Indian government has taken steps toward regulating AI through various policy documents and expert committee recommendations. In 2018, the NITI Aayog released a discussion paper titled *"National Strategy for Artificial Intelligence"*,

identifying privacy and ethics as key areas for AI deployment. The paper stressed the importance of responsible AI, yet stopped short of proposing a statutory framework[38].

In 2021, the Ministry of Electronics and Information Technology (MeitY) released a framework titled *"Responsible AI for All"*, promoting transparency, accountability, and inclusion in AI design. However, these guidelines are non-binding and offer no enforcement mechanism. Moreover, they lack integration with constitutional principles or the Digital Personal Data Protection (DPDP) Act, 2023.

The Justice B.N. Srikrishna Committee Report, which laid the foundation for India's data protection regime, strongly recommended robust privacy safeguards and algorithmic accountability, cautioning against excessive data retention and profiling[39]. Yet, the subsequent DPDP Act diluted many of these safeguards, particularly in exempting state surveillance and failing to regulate AI applications explicitly.

India also lags behind in setting up independent oversight institutions such as AI ethics commissions or data ombudsman bodies, unlike the European Union or Canada. This institutional vacuum hampers effective checks on AI-related privacy violations, especially when state actors are involved.

[36] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

[37] *Internet and Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC 274.

[38] NITI Aayog, *"National Strategy for Artificial Intelligence"*, Government of India, 2018.

[39] Justice B.N. Srikrishna Committee Report, *"A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians"*, Government of India, 2018.

Civil Society and International Advocacy

Beyond the judiciary and government, civil society organizations and legal scholars have played an instrumental role in drawing attention to AI-induced privacy threats. Bodies like the Internet Freedom Foundation and the Centre for Internet & Society have consistently advocated for algorithmic transparency, stronger data protection, and AI governance frameworks based on international human rights standards[40].

Internationally, India's engagement with AI ethics is still nascent, though it has supported UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021), which emphasizes transparency, accountability, and the right to contest algorithmic decisions. Yet, this has not translated into domestic legal commitments. Without binding AI laws or treaty obligations, India remains vulnerable to policy capture and unregulated deployment of AI in sensitive sectors such as finance, policing, and welfare.

Conclusion

The intersection of Artificial Intelligence and the right to privacy under Article 21 presents one of the most urgent legal and constitutional challenges of the digital age. While Indian constitutional jurisprudence—especially post-*Puttaswamy*—recognizes privacy as intrinsic to human dignity and autonomy, the rapid and often opaque deployment of AI technologies threatens to undermine this right through large-scale data collection, profiling, and surveillance.

AI systems today operate in ways that are increasingly invisible, intrusive, and inscrutable. As they expand into domains such as policing, finance, healthcare, and social services, individuals often lose control over how their personal data is collected, processed, or interpreted. The concept of informational autonomy, though acknowledged by courts, has not yet been operationalized through enforceable statutory or institutional frameworks. The Digital Personal Data Protection Act, 2023, while a welcome step, remains limited in scope—particularly in addressing algorithmic harms, non-consensual surveillance, and state exemptions.

Judicial pronouncements have laid a strong normative foundation, but in the absence of AI- specific legislation, their ability to offer meaningful relief remains constrained. Furthermore, policy initiatives such as NITI Aayog's *AI for All* strategy and MeitY's *Responsible AI* framework are advisory and lack legal force.

[40] Internet Freedom Foundation, *"AI and Civil Liberties in India: Need for Ethical Governance"*, Policy Brief, 2021.