LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 3 | Issue 1

2025

AI AND THE RIGHT TO PRIVACY – BALANCING INNOVATION WITH CONSTITUTIONAL PROTECTIONS

Rama Dutt[1]

I. ABSTRACT

This research paper examines the evolving intersection of artificial intelligence (AI) and the right to privacy, focusing on how legal systems can reconcile rapid technological innovation with constitutional protections. The paper analyzes key legal frameworks, landmark judgments, and emerging regulatory approaches to AI globally. It also highlights the ethical implications of surveillance technologies, facial recognition, and predictive algorithms. The study concludes by proposing legal reforms and policy strategies to ensure responsible AI deployment that respects fundamental rights.

II. KEYWORDS

Artificial Intelligence, Privacy Rights, Surveillance, Data Protection, Constitutional Law, Facial Recognition, AI Regulation, Legal Frameworks

III. INTRODUCTION

The emergence of Artificial Intelligence (AI) has fundamentally transformed the technological landscape, influencing almost every facet of modern life. From personalized recommendations on streaming platforms to automated decision-making in healthcare, law enforcement, and finance, AI systems have become an integral part of contemporary society. These technologies rely heavily on large-scale data collection and advanced algorithmic processing, raising complex legal and ethical questions—particularly about the individual's right to privacy.

Privacy is universally recognized as a fundamental human right. It is enshrined in international instruments such as Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, as well as in national constitutions, including Article 21 of the Indian Constitution and the Fourth Amendment to the United States Constitution. In the landmark judgment

[1] Assistant professor, Harlal School of Law, Greater Noida.

 (ISSN: 2583-7753)

of *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court of India explicitly declared the right to privacy as an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution[2]. However, the evolving capabilities of AI—particularly its capacity to gather, analyze, and infer sensitive personal data—have increasingly placed this right under strain.

This conflict between technological innovation and the preservation of individual rights has become one of the most pressing legal challenges of the 21st century. AI applications such as facial recognition software, predictive policing tools, and social media algorithms often operate with minimal transparency and limited regulatory oversight. While they offer efficiency and convenience, they also risk enabling mass surveillance, discriminatory profiling, and data misuse.

This paper aims to investigate the intersection of AI and privacy rights, with a focus on balancing technological advancement with constitutional protections. The research will evaluate the adequacy of existing legal frameworks and regulatory mechanisms in addressing privacy concerns posed by AI. It will also offer a comparative analysis of national and international approaches and provide recommendations for a more robust, rights-based legal framework to govern AI development and deployment.

To structure the inquiry, the following key research questions will be explored:

- How is AI affecting the right to privacy in current practical contexts?
- What are the existing legal protections—constitutional, statutory, and regulatory—available to safeguard privacy from AI-related threats?
- Are these protections sufficient in light of the technological sophistication of modern AI systems?
- What legal reforms or policy interventions are necessary to ensure a rights-compliant approach to AI innovation?

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

By addressing these questions, the paper seeks to contribute to the broader academic and legal discourse on how constitutional democracies can adapt to the demands of the digital age while upholding fundamental civil liberties.

IV. CONSTITUTIONAL FOUNDATIONS OF THE RIGHT TO PRIVACY

The right to privacy, though historically underdeveloped in many constitutional frameworks, has emerged as a core aspect of human dignity and autonomy in modern jurisprudence. As AI technologies become increasingly embedded in public and private life, constitutional protections for privacy face significant challenges. This section explores the legal foundations of privacy in national constitutions—particularly in India and the United States—and examines the pivotal judicial interpretations that have shaped the modern understanding of this right.

A. Privacy in National Constitutions

In India, the right to privacy was not originally enumerated as a fundamental right under the Constitution. However, the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India recognized privacy as a constitutionally protected right under Article 21, which guarantees the right to life and personal liberty[3]. The Court emphasized that privacy is essential to autonomy, dignity, and liberty in a democratic society, and that informational privacy, in particular, must be protected in the digital age.

In contrast, the United States Constitution does not explicitly mention the word "privacy." However, the Fourth Amendment, which protects citizens from unreasonable searches and seizures, has been interpreted to confer certain privacy rights—particularly in contexts involving law enforcement surveillance and data collection. Over time, U.S. courts have relied on this amendment and substantive due process principles to recognize a broader "zone of privacy" in various contexts, including reproductive rights, marriage, and most recently, digital data.

[3] INDIA CONST. art. 21.

B. Judicial Interpretations

1) Puttaswamy v. Union of India (India)

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court of India delivered a landmark ruling in 2017, declaring privacy as a fundamental right under the Constitution[4]. The judgment overruled earlier precedents such as *M.P. Sharma v. Satish Chandra*[5] and *Kharak Singh v. State of U.P.*[6], which had denied such a right. The Court adopted a broad and contemporary interpretation of privacy, including informational privacy, and emphasized that the right must evolve with technological changes.

The Court also recognized the role of data protection, warning against the unchecked use of personal information by both state and private actors. This decision laid the groundwork for India's Digital Personal Data Protection Act, 2023, which aims to regulate the use of personal data in both the public and private sectors.

2) Carpenter v. United States (U.S.)

In *Carpenter v. United States*, the U.S. Supreme Court addressed whether law enforcement could access historical cell-site location information (CSLI) from mobile providers without a warrant[7]. The Court held that the Fourth Amendment protects such data, and that accessing it without a warrant violates an individual's reasonable expectation of privacy.

This ruling marked a significant shift from the earlier "third-party doctrine," which suggested that information voluntarily shared with third parties (like telecom providers) was not protected by the Fourth Amendment. The Court acknowledged that modern digital technologies demand a reassessment of traditional privacy doctrines, especially as AI systems often rely on similar data collection methods.

These constitutional interpretations reveal a growing judicial awareness of the privacy threats posed by emerging technologies. Both India and the U.S. have recognized that

[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[5] *M.P. Sharma v. Satish Chandra*, 1954 S.C.R. 1077 (India).
[6] *Kharak Singh v. State of Uttar Pradesh*, A.I.R. 1963 S.C. 1295 (India).
[7] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

constitutional protections must adapt to address AI-driven data collection and surveillance mechanisms. However, gaps remain in enforcement and scope, especially when AI is used by private corporations outside the direct reach of constitutional safeguards.

V. LEGAL GAPS AND CHALLENGES

While both national and international legal systems have begun to recognize the threats AI poses to privacy, existing frameworks remain largely inadequate to deal with the unique and evolving challenges presented by AI technologies. The rapid development of machine learning algorithms, facial recognition tools, and autonomous decision-making systems has outpaced the ability of lawmakers to provide clear and enforceable guidelines. This section outlines three key areas where legal ambiguity persists: AI-specific risks, the nature of informed consent and algorithmic bias, and the accountability of private versus state actors.

A. Ambiguity in Laws Regarding AI-Specific Risks

Most current privacy and data protection laws—such as India's Digital Personal Data Protection Act, 2023[8]or the EU's General Data Protection Regulation (GDPR)[9]—were designed with traditional data processing models in mind. These laws often fall short when it comes to addressing the autonomous and predictive capabilities of AI systems. For example, the GDPR does contain provisions for automated decision-making (Art. 22), but its language remains vague, and enforcement has been inconsistent[10].

Similarly, India's DPDP Act does not specifically address algorithmic opacity, the use of training data, or automated profiling, all of which are essential concerns in AI regulation. This legal gap leaves room for wide interpretation and creates uncertainty about what is permitted, especially when AI systems are trained using vast datasets that may include personal, sensitive, or even illegally sourced data.

[8] Digital Personal Data Protection Act, No. 22 of 2023, § 2(1), Gazette of India, Aug. 2023
[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
[10] See generally Orla Lynskey, *Deconstructing Data Protection: The 'Added-Value' of a Rights-Based Approach to Privacy?*, 4 Int'l Data Privacy L. 43 (2014).

B. Issues with Consent, Algorithmic Transparency, and Bias

Informed consent is a cornerstone of modern data protection law. However, the concept becomes increasingly problematic in the context of AI, where data collection is often passive, continuous, and inferred rather than explicitly provided. Users may "consent" to broad terms of service without fully understanding how their data will be used by AI systems, particularly in behavioral targeting or recommendation algorithms[11].

Another serious issue is algorithmic bias, where AI systems unintentionally replicate or amplify societal prejudices embedded in training data. This has led to discriminatory outcomes in areas like hiring, policing, and credit scoring. Courts and regulators have begun recognizing these risks, but there remains no uniform legal requirement for algorithmic transparency or explainability, making it difficult for affected individuals to seek recourse[12]. The "black box" nature of many AI models—especially deep learning systems—means that even developers cannot always explain how certain outputs are generated. This lack of transparency undermines accountability and poses challenges for both legal review and public trust.

C. Private vs. State Actors – Who is Accountable?

A further complication arises in determining who bears responsibility for privacy violations committed by AI systems. Traditional constitutional protections often apply only to state actors, leaving private corporations outside their scope. In *Puttaswamy v. Union of India*, while the Court acknowledged the role of private data controllers, the judgment primarily addressed state surveillance[13]. Similarly, the U.S. Constitution does not bind private tech companies unless state action is involved[14].

This distinction is problematic in an era where private companies like Google, Meta, or Amazon collect and process more personal data than many governments. While statutory regulations like the California Consumer Privacy Act (CCPA) attempt to

[11]Solove, Daniel J., *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013).
[12] Barocas, Solon & Selbst, Andrew D., *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671 (2016).
[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[14] *Civil Rights Cases*, 109 U.S. 3 (1883); see also *Manhattan Cmty. Access Corp. v. Halleck*, 139 S. Ct. 1921 (2019).

 (ISSN: 2583-7753)

bridge this gap, they often lack the constitutional weight or enforcement mechanisms necessary to deter misconduct by powerful private entities.

The existing legal landscape is ill-equipped to manage the specific challenges posed by AI technologies. Ambiguity in statutes, ineffective consent mechanisms, opaque algorithms, and accountability gaps between public and private actors leave significant room for misuse. Addressing these challenges requires not only legislative reform but also a fundamental rethinking of legal doctrines and regulatory paradigms in the age of AI.

VI. COMPARATIVE LEGAL FRAMEWORKS

Different jurisdictions have adopted varying strategies to regulate the intersection of AI and privacy. While some rely on comprehensive legal instruments, others have opted for sector-specific or soft-law approaches. A comparative analysis helps to highlight global best practices, legal innovation, and gaps that persist in the regulation of AI and data protection.

A. The European Union – GDPR and the AI Act

The European Union (EU) is considered a global leader in digital rights and privacy protection. The General Data Protection Regulation (GDPR) provides a robust, comprehensive legal framework that regulates the processing of personal data by both private and public entities[15]. It includes provisions specifically addressing automated decision-making and profiling under Article 22, requiring meaningful human intervention and the right to explanation.

In addition, the EU is in the process of finalizing the Artificial Intelligence Act (AI Act), a landmark regulation aimed at classifying AI systems based on their level of risk—ranging from minimal to unacceptable. High-risk AI systems will be subject to strict oversight, documentation requirements, and human oversight[16]. The AI Act

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
[16] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final (Apr. 21, 2021).

 (ISSN: 2583-7753)

complements the GDPR by targeting not only data protection but also transparency, safety, and ethical governance of AI technologies.

B. United States – Sectoral Approach

The United States lacks a unified federal data protection law. Instead, it follows a sectoral approach, regulating privacy through laws like the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and most notably, the California Consumer Privacy Act (CCPA)[17]. The CCPA, and its successor—the California Privacy Rights Act (CPRA)—grants consumers rights to know, delete, and opt out of the sale of their personal data. The Federal Trade Commission (FTC) plays a major role in overseeing privacy and AI-related practices through its enforcement powers under Section 5 of the FTC Act, which prohibits unfair or deceptive trade practices[18]. However, this fragmented framework creates regulatory inconsistencies, leaving many privacy and AI-related practices under-regulated at the federal level.

C. India – Digital Personal Data Protection Act, 2023

India recently enacted the Digital Personal Data Protection Act, 2023 (DPDPA), which aims to establish a legal framework for personal data governance in the country[19]. While the Act includes key principles such as consent, purpose limitation, and data minimization, it lacks specific provisions targeting AI systems. Notably, the law does not include strong requirements on algorithmic accountability, automated decision-making, or rights against AI profiling, unlike the GDPR. The Act has also been criticized for giving broad exemptions to government entities under national security and public interest grounds, which could lead to unchecked data use by state actors[20].

D. China – AI Governance Model

China has adopted a state-driven AI governance model emphasizing national security and social stability. The Personal Information Protection Law (PIPL) and

[17] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq.
[18] 15 U.S.C. § 45 (2023).
[19] Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Aug. 2023.
[20] Vrinda Bhandari & Amba Kak, *India's Data Protection Law: Much Ado About Nothing?*, Internet Freedom Foundation (Aug. 2023).

Cybersecurity Law regulate data collection and processing, with a focus on sovereignty and centralized control[21]. China has also released guidelines for algorithmic recommendation services, requiring platforms to register algorithms and ensure they do not promote harmful or illegal content[22]. While China's approach is more prescriptive and top-down, it lacks independent oversight and rights-based protections, raising concerns about surveillance and authoritarian data control.

VII. EMERGING CASE LAWS AND REGULATORY APPROACHES

As AI technologies continue to evolve, courts and regulators worldwide have begun addressing their legal and ethical implications. This section outlines some of the most notable judicial decisions and international regulatory efforts shaping AI and privacy governance.

A. Notable Court Decisions and Enforcement Actions

In Carpenter v. United States, the U.S. Supreme Court held that accessing cell-site location data without a warrant violates the Fourth Amendment[23]. This marked a significant expansion of digital privacy rights under constitutional law.

In Schrems II, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield Framework due to insufficient protections against U.S. government surveillance[24]. This case emphasized the importance of strong legal safeguards in cross-border data transfers, especially relevant in AI systems that rely on global datasets. The French data protection authority (CNIL) fined Clearview AI for violating GDPR principles by scraping biometric data without consent for facial recognition purposes[25]. Similar enforcement actions are emerging globally against AI systems that collect and process data without adequate legal justification.

[21] Personal Information Protection Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021).
[22] Provisions on the Administration of Algorithmic Recommendation Services, Cyberspace Admin. of China, effective Mar. 1, 2022.
[23] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
[24] *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Schrems II)*, Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020).
[25] CNIL, *Clearview AI Inc. Sanctioned for Breaching GDPR*, Oct. 20, 2022.

B. International Bodies and Ethical Guidelines

Global organizations have also recognized the urgent need to establish standards for AI ethics and governance:

The Organisation for Economic Co-operation and Development (OECD) adopted OECD AI Principles in 2019, promoting trustworthy AI systems that respect human rights and democratic values[26]. The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) is one of the first global instruments to address AI ethics, emphasizing human oversight, inclusiveness, and environmental sustainability[27]. The G20 and G7 have also issued joint communiqués urging ethical AI development and better alignment of national frameworks, although these remain non-binding. A comparative and jurisprudential perspective reveals a diverse and fragmented global landscape. While some jurisdictions like the EU lead in rights-based approaches, others focus on sectoral or authoritarian models. As AI continues to evolve, the need for harmonized, transparent, and enforceable legal standards becomes increasingly critical.

VIII. ETHICAL AND PHILOSOPHICAL DIMENSIONS

As artificial intelligence becomes deeply embedded in society, it raises critical ethical and philosophical questions that go beyond legal compliance. These dimensions influence how laws are framed and interpreted and are essential for balancing technological advancement with fundamental rights.

A. Autonomy, Dignity, and Informed Consent in the AI Age

Autonomy and dignity form the bedrock of human rights jurisprudence and democratic governance. In the context of AI, these values are challenged when personal data is harvested, analyzed, and used without meaningful consent. As AI systems make increasingly complex decisions—from credit scoring to predictive

[26] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (May 22, 2019).
[27] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 41 C/Res. 41, Nov. 24, 2021.

policing—individuals may be subjected to outcomes without understanding how or why those decisions were made[28].

The traditional notion of informed consent becomes problematic in AI ecosystems, where consent is often bundled in lengthy privacy policies or assumed through platform use. Scholars like Daniel Solove have argued that the self-management model of consent is a "fiction" in digital contexts[29]. Without explainability and transparency in algorithms, users are deprived of the ability to make informed choices, effectively undermining their autonomy.

B. Surveillance Capitalism and Commodification of Data

Coined by Shoshana Zuboff, the term "surveillance capitalism" describes an economic system where human experience is mined for behavioral data, which is then used to predict and influence behavior for profit[30]. Tech giants like Google, Meta, and Amazon rely on vast data ecosystems to fuel AI engines—raising ethical concerns about consent, commodification, and exploitation. In this model, data becomes currency, and individuals are reduced to data points. This not only threatens individual dignity but also distorts the social contract. The lack of equitable data governance exacerbates power asymmetries, where corporations control narratives, behavior, and even political discourse through AI-powered platforms[31].

C. Role of Ethics in Lawmaking

While law provides the enforceable boundaries, ethics provides the moral compass. Ethical AI frameworks stress principles such as beneficence, non-maleficence, autonomy, and justice. These have been reflected in global guidelines like the OECD AI Principles[32] and UNESCO's AI Ethics Recommendations[33]. However, for ethics to influence law meaningfully, it must be embedded into legislative processes. This

[28] Sandra Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 Int'l Data Privacy L. 76 (2017).
[29] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013).
[30] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).
[31] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford Univ. Press 2019).
[32] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (May 22, 2019).
[33] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 41 C/Res. 41 (2021).

includes ethical impact assessments, public consultations, and interdisciplinary policy-making that includes ethicists, technologists, and legal scholars. Ethics should not remain a "soft law" alternative but evolve into binding legal norms where necessary, especially for high-risk AI systems.

IX. CONCLUSION AND SUGGESTIONS

A. Summary of Key Findings

The intersection of artificial intelligence and the right to privacy presents complex legal, ethical, and societal challenges. While AI offers transformative benefits in healthcare, education, governance, and beyond, it also introduces profound risks to privacy, autonomy, and equality. Current legal frameworks, though evolving, are largely reactive rather than proactive, struggling to keep pace with technological advancements.

Notable gaps include:

- Lack of AI-specific legal instruments,
- Insufficient algorithmic transparency,
- Weak enforcement mechanisms,
- Limited protection against private-sector surveillance.

Simultaneously, global jurisprudence and policy efforts (e.g., GDPR, AI Act, PIPL, CCPA) indicate a shift toward principle-based governance, yet a global consensus remains elusive.

B. Suggestions

To build a sustainable and rights-respecting AI ecosystem, the following measures are recommended:

1. Enact Clear, AI-Specific Legislation

Governments must introduce dedicated laws for AI governance, addressing issues like automated decision-making, profiling, deepfakes, and biometric surveillance.

These laws should draw from best practices globally but be tailored to national constitutional values[34].

2. Mandate Transparency and Explainability of Algorithms

Legal mandates should require algorithmic transparency and explainability, especially for high-impact decisions (e.g., policing, hiring, credit). Explainable AI (XAI) not only supports individual rights but also improves accountability and trust in systems[35].

3. Strengthen Data Protection Authorities

Independent data protection authorities (DPAs) must be empowered with technical expertise, financial resources, and legal mandates to investigate AI-related privacy violations and issue binding orders[36].

4. Encourage Ethical AI Development and Public Awareness

Governments and institutions must promote ethical AI design, including fairness audits, impact assessments, and AI literacy campaigns. Ethical certifications and incentives for responsible innovation can promote industry self-regulation aligned with public interest[37].

[34] Vidushi Marda & Divij Joshi, *Artificial Intelligence in India: A Rights-Based Perspective*, Article 19 (2019).
[35] Finale Doshi-Velez & Been Kim, *Towards a Rigorous Science of Interpretable Machine Learning*, arXiv:1702.08608 [cs.AI] (2017).
[36] Graham Greenleaf, *Global Data Privacy Laws 2023: 162 National Laws & Many Bills*, (2023) 177 Privacy Laws & Business Int'l Rep.
[37] AI Now Institute, *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability* (2018).

 (ISSN: 2583-7753)