International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Right to Privacy and The Expanding Horizon of Artificial Intelligence : A Constitutional Concern in India

Dr. KeshavNand

Assistant Professor & Head Department of Laws, The ICFAI University Himachal Pradesh

Nikita Dhiman

Research Scholar, Faculty of Law, The ICFAI University, Himachal, Pradesh.

Abstarct - Artificial Intelligence (AI) is playing an increasingly important role in India's digital growth. It is utilized across various sectors, including government services, banking, healthcare, education, and everyday life. Although AI provides numerous advantages such as quicker services, enhanced decision-making, and increased accessibility, it also brings significant issues regarding individuals' privacy.

The Supreme Court of India acknowledged the right to privacy as a fundamental right in the significant case of Justice K.S. Puttaswamy (Retd.) v. Union of India. Nonetheless, safeguarding this right has become increasingly difficult due to the emergence of AI, extensive data gathering, and automated decision-making processes. This paper explores the evolution of privacy rights in India, starting with earlier cases like M.P. Sharma and Kharak Singh, where privacy was inadequately acknowledged, and progressing to the Puttaswamy ruling, which solidly affirmed privacy as a constitutional right. The article also explores how AI poses risks to privacy via extensive data gathering, opacity in decision processes, biased algorithms, and widespread surveillance. These challenges frequently impact vulnerable and marginalized populations more intensely.

The research additionally assesses India's existing legal and policy structure, comprising the Digital Personal Data Protection Act, 2023, the suggested Digital India Act, and policy suggestions released by NITI Aayog. It highlights various deficiencies in these approaches, especially in terms of accountability for AI systems and the necessity for autonomous regulatory supervision.
Through a comparison of India's strategy with legal advancements in the European Union, United States, China, and the United Kingdom, the paper contends that India ought to implement a rights-oriented framework for AI governance. This framework ought to incorporate explicit protections for privacy, clarity in AI decision-making processes, independent oversight systems, technologies that safeguard privacy, and enhanced public involvement.
The paper concludes that even as India strives to be a global leader in artificial intelligence, progress in technology should be paired with robust safeguarding of constitutional principles. AI must be created and utilized in a way that fosters personal freedom, human dignity, equality, and democratic values instead of threatening them.

1. INTRODUCTION

The term 'privacy' originates from the Latin word 'Privatus', which signifies isolation, restriction, personal matters, or uniqueness. There is no universally accepted definition of privacy but According to Black's Law Dictionary[1], privacy is defined as 'the right to be let alone; the right of a person to be free from unwarranted publicity; and the right to live without unwarranted interference by the public in matters that do not necessarily concern them.' Particularly in the United Kingdom and the United States, it is viewed as a protection against governmental, corporate, and individual intrusions into personal privacy. In some countries, these protections are guaranteed by law. For instance, tax laws in numerous nations require citizens to disclose their income and other private financial information to the government. Especially when laws necessitate public disclosure of matters that other nations and cultures consider private, freedom of expression may conflict with individual privacy regulations in certain countries. The right to privacy has evolved alongside the development of the humanist tradition. This right is a fundamental human right that is

[1] "Privacy" Black's Law dictionary.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

crucial for the operation of a free and democratic society. It includes the individual's right to keep personal information, communications, and activities confidential and safeguarded from unauthorized intrusion. The significance of the right to privacy can be appreciated through various aspects: Privacy is intimately connected to personal autonomy, which is the capacity to make choices about one's own life without interference or coercion. The liberty to make decisions regarding one's own relationships, beliefs, and preferences, among other aspects, is a vital element of the right to privacy. It is essential because it empowers individuals to make choices about their own lives.

The right to privacy is fundamental for safeguarding individuals' dignity and security. It enables individuals to develop their distinct identities and protect their reputations. Privacy shields individuals from unwarranted examination, judgement, and stigma, allowing them to express themselves openly and freely without the constant fear of illegal intrusion or exposure. Both physical and mental safety rely on an individual's capacity to uphold privacy. It serves as a means for individuals to protect themselves from harassment, violence, and various threats. A notable benefit of safeguarding individuals' privacy is that it complicates identity theft for criminals by keeping personal financial and medical details, along with physical addresses, confidential. Trust among individuals, organisations, and governments flourishes when personal data is kept private. When individuals are assured that they can confide in one another regarding their personal information, they are more inclined to communicate openly, seek help when necessary, and share sensitive information when required. The right to privacy is frequently viewed as a fundamental human right. Although it is not explicitly mentioned, it can be deduced from various Articles of the Universal Declaration of Human Rights (UDHR), including Article 12, which asserts that 'no one shall be subjected to arbitrary interference with his privacy.' Other international human rights agreements, such as the International Covenant on Civil and Political Rights (ICCPR), also safeguard the right to privacy. The right to privacy is among the numerous human rights that the United Nations (UN) strives to promote and protect.

2. HISTORICAL DEVELOPMENT OF PRIVACY LAW IN THE DIGITAL AGE

The legal history of privacy in India cannot be confined to statutes enacted after the internet, because the underlying claim has older moral, social and constitutional roots. Privacy first appeared as an interest in restraint, secrecy, household autonomy, honour and personal dignity, rather than as a named legal entitlement. Its modern form emerged only when personal information became capable of extraction, storage, transfer and computation by public and private actors. The digital age, therefore, did not create the need for privacy; it altered the scale, speed and legal consequences of its violation.[2]
The older legal imagination treated personal boundaries as part of ordered social life, while modern law treats them as part of individual liberty and dignity. This movement reflects a gradual shift from community-regulated secrecy to rights-based protection against intrusion, surveillance and informational domination. The change is especially significant in India because privacy developed through several overlapping sources: ancient ethical literature, medieval social practice, colonial communication controls, constitutional liberty and later data-protection legislation. Each stage contributed a distinct legal vocabulary, even when the word privacy itself was absent.[3]

Digital technology has made privacy both more visible and more vulnerable. A physical search, intercepted letter or overheard conversation affects a limited sphere; a digital record may expose location, behaviour, association, preference, identity and future risk.

- **Civilisational foundations of privacy in ancient Indian thought**

Ancient Indian thought did not frame privacy as a modern subjective right, but it recognised protected spaces of life, counsel and reputation. Its concern lay in social discipline, restrained speech, household sanctity and controlled access to intimate knowledge.[4]

- **Privacy, Secrecy and social order in medieval Indian legal culture**

Medieval legal culture preserved many older concerns but placed them within plural normative orders, including royal authority, religious law, caste practice and commercial custom. Privacy remained embedded in honour, household order, gendered seclusion and confidential dealings.[5]

---

2 Daniel J. Solove, *Understanding Privacy* 118 (Harvard University Press, Cambridge, 1st edn., 2008).
3 Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy", 4 *Harvard Law Review* 193 (1890).
4 Fundamental Right to Privacy, *available at:* https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/ (last visited on May 3, 2026).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

- **Colonial era foundations of communications control and personal autonomy**

  Colonial rule altered privacy by creating centralised systems for postal, telegraphic, police and administrative intelligence. Communication became a governable object, and personal autonomy remained subordinate to public order, empire and executive discretion.[6]

- **Constitutional emergence of privacy in post-Independence India**

  After Independence, privacy moved from inherited fragments toward constitutional meaning. The Constitution supplied a rights-based vocabulary of liberty, dignity, equality and lawful restraint, allowing privacy to be understood as part of legal personhood.[7]

- **Transformation of privacy in the digital Datafication and Artificial Intelligence era**

  The digital era recast privacy by converting behaviour into data and data into governable intelligence. The legal issue moved from secrecy alone to control, accountability, consent, retention, profiling and automated inference.[8]

3. LEGAL AND REGULATORY FRAMEWORK GOVERNING PRIVACY AND AI

Privacy and AI generate a legal tension between informational autonomy, computational inference, public regulation, and market deployment. Automated systems can classify, predict, rank, recommend, authenticate, and surveil persons through data that may appear impersonal at the point of collection but may become identifiable through aggregation.[9] Indian law does not treat this field through one self-contained AI statute. It proceeds through constitutional rights, data protection norms, information technology legislation, cybersecurity directions, criminal liability, criminal process, and evidentiary rules that determine when digital material can be acted upon in courts and by public authorities.[10] Privacy and AI generate a legal tension between informational autonomy, computational inference, public regulation, and market deployment. Automated systems can classify, predict, rank, recommend, authenticate, and surveil persons through data that may appear impersonal at the point of collection but may become identifiable through aggregation.[11] Indian law does not treat this field through one self-contained AI statute. It proceeds through constitutional rights, data protection norms, information technology legislation, cybersecurity directions, criminal liability, criminal process, and evidentiary rules that determine when digital material can be acted upon in courts and by public authorities.[12]

The framework is fragmented but legally connected. Constitutional provisions supply the baseline of equality, freedom, liberty, remedies, and legislative competence. The Digital Personal Data Protection Act, 2023 creates the principal private and public data-processing regime. The Information Technology Act, 2000 and its rules regulate electronic records, cybersecurity, intermediaries, and online content duties. The Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023 then deal with offences, investigation, trial, and proof. AI is governed through this composite legal structure rather than through a single code.[13]

---

5 Ruby Lal, "Historicizing the Harem: The Challenge of a Princess's Memoir", 30 *Feminist Studies* 590 (2004).
6 C.A. Bayly, *Empire and Information: Intelligence Gathering and Social Communication in India, 1780-1870* 123 (Cambridge University Press, Cambridge, 1st edn., 1996).
7 H.M. Seervai, *Constitutional Law of India: A Critical Commentary* 176 (N.M. Tripathi, Bombay, 4th edn., 1991).
8 DPDP Rules, 2025 Notified, *available at:* https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655 (last visited on May 1, 2026).
9 Gautam Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography", 26 *National Law School of India Review* 127 (2014).
10 Gautam Bhatia, *The Transformative Constitution* 73 (HarperCollins, Noida, 1st edn., 2019).
11 Gautam Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography", 26 *National Law School of India Review* 127 (2014).
12 Gautam Bhatia, *The Transformative Constitution* 73 (HarperCollins, Noida, 1st edn., 2019).
13 Sheshadri Chatterjee, "Is Data Privacy a Fundamental Right in India? An Analysis and Recommendations from Policy and Legal Perspective", 61 *International Journal of Law and Management* 170 (2019).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

A) Indian Constitutional And Data Protection Framework

Indian privacy law begins with constitutional discipline and then moves into statutory governance of digital personal data. The framework controls State power, guides legislative design, and regulates private actors whose data-processing choices affect autonomy, dignity, access, and informational self-determination.[14]

The Constitution of India, 1950

The constitutional plane gives privacy and AI regulation its public-law foundation. Articles 14, 19, and 21 govern equality, freedoms, and liberty, while Articles 32 and 226 provide remedial supervision. Legislative competence under Articles 245, 246, 248, and 253 permits Parliament to enact national digital governance measures, including laws with extra-territorial operation where constitutionally supported. Article 245 states "Parliament may make laws for the whole or any part of the territory of India", and this supports national regulation of digital systems whose effects cross State boundaries.[15]

B) Digital Personal Data Protection Act, 2023

The central statutory instrument recognises a dual object: protection of individual personal data and processing for lawful purposes. Its long title describes an Act for processing digital personal data in a manner that recognises "both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes." The Act's commencement has been staggered by notification, making commencement status legally material when duties and enforcement powers are assessed.[16]

Digital Personal Data Protection Rules, 2025

The Rules translate the Act into operational duties. They were made under Section 40 of the Act, and the official notification states that Rules 1, 2 and 17 to 21 came into force on publication, Rule 4 after one year, and Rules 3, 5 to 16, 22 and 23 after eighteen months. This phased commencement is legally significant because notice, consent, security, and Board procedure duties mature at different points.[17]

C) Indian Information Technology and Cyber Security Framework

The information technology framework governs digital records, authentication, cyber incidents, intermediary conduct, and State powers over online information. It connects privacy and AI to platform responsibility, cybersecurity readiness, lawful interception, blocking, and recognition of electronic transactions.[18]

Information Technology Act, 2000

The Act supplies the legal infrastructure for electronic records, electronic signatures, cybersecurity, cyber contraventions, and intermediary liability. Its relevance to AI arises because automated systems operate through computer resources, electronic records, data storage, communications, and online publication. It does not create a complete AI code, but it determines whether digital records have legal recognition, whether unauthorised access attracts liability, whether platforms can claim safe harbour, and whether State authorities may compel interception, monitoring, decryption, or blocking. India Code records it as Act Number 21 of 2000.[19]

Information Technology Rules, 2011

The 2011 sensitive personal data rules created the earlier sector-neutral privacy layer under Section 43A. They required privacy policies, consent for sensitive personal data, purpose limitation, disclosure restrictions, transfer safeguards, grievance officers, and

---

[14] Data Protection Laws in India, *available at:* https://www.dlapiperdataprotection.com/?c=IN&t=law (last visited on May 3, 2026).
[15] M.P. Jain, *Indian Constitutional Law* 189 (LexisNexis, Gurgaon, 8th edn., 2018).
[16] Abhishek Singh, Anusha, "The Digital Personal Data Protection Act, 2023: An Ambitious Government Step Towards Ensuring Its Wide Reach", 70 *Indian Journal of Public Administration* 502 (2024).
[17] Graham Greenleaf, "Rules Expand India's Data Privacy Law, but Slowly", 185 *Privacy Laws & Business International Report* 1 (2026).
[18] Vakul Sharma, *Information Technology Law and Practice* 158 (Universal Law Publishing, Delhi, 5th edn., 2016).
[19] Loshika Sharma, "Digital Privacy in India", 12 *International Journal for Innovative Engineering and Management Research* 1323 (2023).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

reasonable security practices. Rule 5 required consent before collection and limited collection to lawful and necessary purposes, while Rule 8 dealt with security practices. Even after the DPDP Act's broader personal data regime, these rules remain doctrinally important for understanding the transition from sensitive-data protection to a comprehensive data fiduciary model.[20]

Information Technology Rules, 2021

The 2021 Rules regulate intermediaries and digital media duties under the Information Technology Act, 2000. The updated official text records the title as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and notes that the Rules were updated as on 10 February 2026. Their relevance to AI lies in intermediary due diligence, grievance redressal, significant intermediary duties, proactive technical measures, and the newer regulatory treatment of synthetically generated information.[21]

D) CERT-In Directions, 2022

The cybersecurity framework is completed by the statutory role of the Indian Computer Emergency Response Team under Section 70B of the Information Technology Act, 2000 and the 2022 Directions. These Directions require reporting of specified cyber incidents, preservation of logs, and cooperation with incident response. For AI, cybersecurity is not ancillary. Training data theft, model exfiltration, adversarial attacks, data poisoning, credential compromise, and prompt leakage may produce privacy breaches and operational harm. Incident reporting therefore supports public oversight of technical failures affecting personal data and digital infrastructure.

E) Indian Criminal Procedure and Evidence Framework

Criminal and evidentiary law addresses privacy and AI harms after wrongful conduct occurs. It defines offences, enables investigation, regulates search and seizure, recognises electronic proceedings, and determines how electronic records are proved before courts.[22]

Bharatiya Nyaya Sanhita, 2023

The penal framework is relevant because AI-enabled harm frequently appears as deception, personation, forgery, sexual privacy violation, stalking, extortion, defamation, or circulation of obscene material. The Bharatiya Nyaya Sanhita, 2023 came into force on 1 July 2024 and its text expressly extends to offences targeting computer resources located in India. Section 2 also expands “document” to include electronic and digital records, allowing digitally created instruments, deepfake materials, forged files, and automated outputs to be legally assessed as documents where their evidentiary use is material.[23]

Bharatiya Nagarik Suraksha Sanhita, 2023

Procedure determines whether privacy-protective criminal law can be enforced without creating unchecked investigative intrusion. The Bharatiya Nagarik Suraksha Sanhita, 2023 came into force on 1 July 2024 and consolidates criminal procedure. It contains provisions for electronic complaints, investigation, production of documents and electronic communication, search, seizure, and electronic proceedings. AI-related offences often depend on fast preservation of logs, devices, cloud accounts, source files, and communications. Procedure therefore must balance investigative necessity with legality, record integrity, and judicially controlled compulsion.[24]

Bharatiya Sakshya Adhiniyam, 2023

The evidentiary framework determines whether electronic records, digital signatures, automated logs, metadata, and forensic outputs can be admitted and weighed. The Bharatiya Sakshya Adhiniyam, 2023 came into force on 1 July 2024 and expressly includes electronic and digital records within the concept of documents. This is crucial for AI because proof may depend upon

---

[20] Government Has Issued Multiple Advisories Emphasizing the Observance of Due Diligence Obligations Under the IT Act and IT Rules, *available at:* https://www.pib.gov.in/PressReleasePage.aspx?PRID=2245053 (last visited on April 27, 2026).

[21] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data", 47 *Seton Hall Law Review* 995 (2017).

[22] K.N. Chandrasekharan Pillai, *R.V. Kelkar's Criminal Procedure* 74 (Eastern Book Company, Lucknow, 7th edn., 2021).

[23] S. M. Aamir Ali, Pritha Mukhopadhyay, "Bharatiya Nyaya Sanhita: Decolonizing Criminal Law or Colonial Continuities", 62 *International Annals of Criminology* 406 (2024).

[24] R.V. Kelkar, *R.V. Kelkar's Lectures on Criminal Procedure: Based on Bharatiya Nagarik Suraksha Sanhita, 2023* 91 (Eastern Book Company, Lucknow, 7th edn., 2025).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

system logs, hash values, device reports, model-generated outputs, provenance metadata, synthetic content labels, and expert explanation of automated processes.[25]

4. COMPARATIVE COUNTRY FRAMEWORKS

Comparative legal materials show three regulatory models: rights-based data protection, risk-based AI control, and sectoral consumer protection. These models differ in legislative form,

but each addresses consent, transparency, automated processing, high-risk systems, data security, enforcement, and cross-border governance.[26]

a) European Union

The European Union framework combines comprehensive data protection with a distinct AI statute. The General Data Protection Regulation, 2016 governs personal data processing through principles, lawful bases, rights, impact assessment, security, transfer controls, and penalties. The Artificial Intelligence Act, 2024 adds system-specific governance for prohibited, high-risk, transparency-sensitive, and general-purpose AI systems. This dual structure is legally significant because privacy harms and AI harms are related but not identical. Data protection addresses information processing, while AI regulation addresses model conduct, risk management, oversight, documentation, and accountability across the AI lifecycle.[27]

b) United Kingdom

The United Kingdom framework relies on the United Kingdom General Data Protection Regulation, 2018, read with the Data Protection Act, 2018. It does not create a single horizontal AI statute equivalent to the European Union Artificial Intelligence Act, 2024. Its legal position is therefore shaped by data protection duties, sectoral regulators, equality obligations, consumer protection, public law standards, and guidance on AI assurance. The model remains privacy-centred in formal legal terms, but its application to AI depends on whether a system processes personal data, produces legal effects, or creates comparable significant impact.[28]

c) United States of America

The United States framework is fragmented, combining federal privacy statutes, consumer protection enforcement, state privacy law, executive policy, and technical risk-management standards. It lacks a single comprehensive federal privacy statute or horizontal AI Act of general application. The legal pattern is therefore sectoral and enforcement-driven. Privacy risks from AI may be addressed through unfair or deceptive practices, agency-specific obligations, public-sector record rules, state consumer rights, and risk guidance. This structure gives regulators flexibility, but it also creates uneven protection where AI systems cross sectors, jurisdictions, and data categories.[29]

5. JUDICIAL RESPONSES TO PRIVACY CHALLENGES IN ARTIFICIAL INTELLIGENCE

1. **Olmstead v. United States**[30], the Supreme Court of the United States considered whether federal wiretapping of telephone conversations, conducted without physical entry into the defendants' premises, violated the Fourth Amendment. The majority held that no search or seizure had occurred because there was no physical trespass upon the defendants' property and no seizure of tangible papers or effects. The dissenting opinions, particularly those addressing the right to be let alone, later became influential. The decision's relevance to AI privacy lies in its formalism. It shows the insufficiency of a property-confined model where surveillance operates through networks, signals, databases, and machine analysis rather than physical entry.

---

[25] Anju Sinha, "Digital Proofs and Legal Admissibility: Understanding Electronic Evidence under the Bharatiya Sakshya Adhiniyam", 25 *Revista Electronica De Veterinaria* 28 (2024).

[26] Daniel J. Solove, Paul M. Schwartz, *Privacy Law Fundamentals* 112 (International Association of Privacy Professionals, Portsmouth, 7th edn., 2024).

[27] Paul De Hert, Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?", 32 *Computer Law & Security Review* 179 (2016).

[28] Anastasia Choromidou, "EU Data Protection Under the TCA: The UK Adequacy Decision and the Twin GDPRs", 11 *International Data Privacy Law* 388 (2021).

[29] Daniel J. Solove, Woodrow Hartzog, "The FTC and the New Common Law of Privacy", 114 *Columbia Law Review* 583 (2014).

[30] 277 *U.S.* 438 (1928).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

2. **Katz v. United States**[31], the Supreme Court of the United States examined the warrantless electronic recording of conversations made from a public telephone booth. The Court held that the Fourth Amendment protects people and not merely places, and that electronic surveillance of the defendant's conversation constituted a search. Justice Harlan's concurring opinion supplied the structured formulation that became the dominant test for privacy expectation. The decision is central to AI privacy because it permits judicial scrutiny of non-trespassory monitoring. It allows courts to ask whether automated capture, model training, or predictive analysis invades a protected expectation, even when no physical space is entered.

3. **Smith v. Maryland**[32], the Supreme Court of the United States considered whether police installation of a pen register at a telephone company, recording numbers dialled from the defendant's phone, constituted a search. The Court held that the defendant had no legitimate expectation of privacy in numbers voluntarily conveyed to the telephone company. The decision formed the third-party exposure rule for metadata. Its AI relevance is contested. While it supports state access to non-content transactional data, it inadequately accounts for modern analytic aggregation, where innocuous metadata can disclose associations, habits, movements, and behavioural predictions with greater precision than content.

4. **People's Union for Civil Liberties v. Union of India**[33], the Supreme Court of India examined telephone tapping under executive authorisation and its compatibility with the right to privacy. The Court accepted that telephone conversation is an important facet of private life and that interception must be legally controlled. It did not invalidate the statutory power, but prescribed procedural safeguards to prevent arbitrary use. The decision is legally significant for AI privacy because it links surveillance validity to structured authorisation, reasoned necessity, time limits, and review. These principles remain applicable where automated monitoring, communication analytics, or voice-data processing is deployed by public authorities.
5. **District Registrar and Collector, Hyderabad v. Canara Bank**[34], the Supreme Court of India considered whether statutory powers allowing inspection and seizure of bank records without adequate safeguards violated privacy protections. The Court held that privacy is not lost merely because documents are held by a bank, and that compulsory access must satisfy constitutional limits. The decision's legal relevance to AI is substantial. It resists the claim that third-party custody extinguishes privacy and supports scrutiny of state access to financial and documentary datasets. It also anticipates the problem of algorithmic profiling through records that appear administrative but disclose personal life when aggregated.
6. **Selvi v. State of Karnataka**[35], the Supreme Court of India considered the involuntary use of narco-analysis, polygraph examination, and brain electrical activation profile tests during criminal investigation. The Court held that compulsory administration of these techniques violated personal liberty and the protection against testimonial compulsion. It reasoned that such methods intrude into mental privacy and undermine the voluntariness required for evidentiary use. The decision is critical for AI privacy because it protects cognitive autonomy against technologically mediated extraction. It also limits investigative claims that scientific or automated tools can override consent, bodily integrity, and the right to remain silent.
7. **United States v. Jones**[36], the Supreme Court of the United States held that attaching a GPS device to a vehicle and using it to monitor movements constituted a search under the Fourth Amendment. The material facts concerned law-enforcement placement of a tracking device on a vehicle without valid warrant authority, followed by prolonged monitoring. The Court treated the vehicle as an "effect" and relied on physical trespass for the purpose of obtaining information. Its doctrinal relevance for artificial intelligence lies in recognising that digital surveillance acquires constitutional significance when technology enables detailed behavioural reconstruction through accumulation, even where individual movements occur in public spaces.
8. **Riley v. California**[37], the Supreme Court of the United States held that police generally must obtain a warrant before searching digital information on a cellphone seized from an arrested person. The facts involved searches of mobile phones after arrest, with law enforcement relying on the search-incident-to-arrest doctrine. The Court distinguished physical objects from digital devices because of storage capacity, breadth of personal information, and access to remote records. Its doctrinal relevance for artificial intelligence lies in recognising that digital repositories permit inferential reconstruction of life, making ordinary arrest powers insufficient safeguards against algorithmic search.
9. **R. v. Spencer**[38], the Supreme Court of Canada held that a person may have a reasonable expectation of privacy in subscriber information linking an internet account to online activity. Police had requested subscriber details from an internet service provider

[31] 389 *U.S.* 347 (1967).
[32] 442 *U.S.* 735 (1979).
[33] (1997) 1 SCC 301.
[34] (2005) 1 SCC 496.
[35] (2010) 7 SCC 263.
[36] 565 *U.S.* 400 (2012).
[37] 573 *U.S.* 373 (2014).
[38] 2014 SCC 43, [2014] 2 S.C.R. 212.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

without prior judicial authorisation during an investigation involving online file sharing. The Court rejected a narrow view of subscriber data as merely identifying information. Its doctrinal relevance for artificial intelligence lies in recognising that identity linkage enables deeper retrospective analysis of digital conduct and may expose anonymous activity to state reconstruction.

10. **Maximillian Schrems v. Data Protection Commissioner**[39], the Court of Justice of the European Union invalidated the European Commission's Safe Harbour adequacy decision concerning transfers of personal data to the United States. The dispute arose after a complaint that Facebook Ireland transferred user data to the United States, where public authorities could access it under surveillance programmes. The Court held that adequacy requires effective protection essentially equivalent to European Union law. Its doctrinal relevance for artificial intelligence lies in subjecting data-export architectures to rights-based scrutiny where foreign access may affect privacy, remedy, and data protection.
11. **Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others**[40], the Supreme Court of India held that privacy is a constitutionally protected right under Part III of the Constitution of India. The reference arose from challenges involving biometric identity and the State's claim that privacy lacked fundamental-right status. The Court recognised privacy as intrinsic to life, liberty, dignity, autonomy, and informational self-determination. Its doctrinal relevance for artificial intelligence lies in providing the constitutional foundation for contesting data-intensive governance, biometric processing, automated profiling, and disproportionate surveillance by public authorities.
12. **Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems**[41]**,** the Court of Justice of the European Union examined transfers of personal data from the European Union to the United States through standard contractual clauses and the Privacy Shield adequacy framework. The material issue was whether transferred data received protection essentially equivalent to that guaranteed within the Union, given access by United States intelligence authorities and limited redress for non-citizens. The Court invalidated Privacy Shield and sustained standard clauses only where supplementary assessment could secure equivalent protection. Its relevance to artificial intelligence lies in treating transnational data flows as legally conditioned by surveillance risk, not by contractual consent alone.
13. **Re Facebook Biometric Information Privacy Litigation**[42], the United States District Court for the Northern District of California reviewed a class settlement arising from allegations that Facebook's tag-suggestion technology created facial templates from user photographs without legally sufficient consent. The Court approved a substantial settlement after examining class treatment, notice, objections, attorney fees, and relief for affected users. The decision is relevant to artificial intelligence because it treats facial-template extraction as a mass privacy injury suitable for collective adjudication, while placing judicial responsibility on settlement fairness where biometric processing operates at platform scale.
14. **Meta Platforms Inc. v. Bundeskartellamt**[43], the Court of Justice of the European Union examined the relationship between competition authority review and GDPR compliance in the context of platform data combination. The dispute concerned Meta's combining of user data from Facebook, other group services, and third-party websites or apps for personalised advertising and service operation. The court held that a competition authority may consider GDPR compatibility where necessary for assessing abuse of dominance, while respecting the powers of data-protection authorities. The ruling is significant because AI-driven profiling often depends on cross-service data aggregation, making market power and privacy intrusion legally interdependent rather than separate regulatory questions.
15. **Hurbain v. Belgium [GC]**[44], the European Court of Human Rights assessed a civil order requiring the publisher of Le Soir to anonymise a name in an online archive concerning an old fatal road accident. The Article had been lawful when published, but continuing digital accessibility revived reputational harm long after the event. The Court held that anonymisation did not breach press freedom because the measure preserved the archive while reducing identifiability. The judgment treats digital memory as a distinct privacy challenge, where searchability, time, rehabilitation, and proportional editorial burden shape the balance between public record and private life.
16. **Zellmer v. Meta Platforms, Inc**.[45], the United States Court of Appeals for the Ninth Circuit considered whether face signatures created from photographs of a non-user amounted to protected biometric identifiers or biometric information under Illinois biometric privacy law. The plaintiff alleged that friends uploaded his photographs and that Meta generated facial signatures without consent. The Court affirmed judgment for Meta because the record did not show that the face signatures

[39] Case C-362/14, ECLI:EU:C:2015:650.
[40] (2017) 10 SCC 1.
[41] Case C-311/18, ECLI:EU:C:2020:559.
[42] 522 F. Supp. 3d 617 (N.D. Cal. 2021).
[43] Case C-252/21, ECLI:EU:C:2023:537.
[44] App. No. 57292/16, ECHR 2023.
[45] 104 F.4th 1117 (9th Cir. 2024).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

could identify the plaintiff. The decision narrows biometric privacy liability where a derived facial representation is not proven to possess identifying capacity, while leaving non-user protection conceptually open.

6. CRITICAL EXAMINATION OF EMERGING PRIVACY ISSUES AND CHALLENGES IN ARTIFICIAL INTELLIGENCE

Artificial intelligence converts ordinary digital interaction into legal exposure by making personal information continuously observable, inferable, and reusable. Indian privacy discourse must therefore examine not only unauthorised disclosure, but also lawful processing that silently alters autonomy, dignity, equality, and decisional control.[46]

Datafication, Collection asymmetry, And consent vulnerability:-

AI systems enlarge the legal significance of data collection because minor acts of disclosure become inputs for prediction, training, classification, and future reuse. The privacy concern lies in unequal informational power, where individuals supply fragments while entities construct durable profiles from aggregated traces.[47]

Profiling, Inferential Analytics, And Autonomy Harms

AI privacy harm increasingly arises from what systems infer rather than what individuals disclose. Profiling converts behavioural fragments into assessments of risk, preference, emotion, credibility, health, productivity, or susceptibility, thereby affecting autonomy without direct intrusion into private spaces.[48]

Opacity, Explainability deficits, And Accountability Challenges

AI privacy regulation faces a central evidentiary problem: the individual may suffer adverse treatment without knowing what data was used, how it was weighted, who processed it, or whether the result came from lawful, accurate, and proportionate processing.[49]

Bias, Discrimination , And Collective Privacy Harms

AI privacy concerns intersect with equality because surveillance and profiling do not burden all persons equally. Dataset design, proxy variables, unequal visibility, and administrative dependency may expose marginalised groups to greater scrutiny, weaker choice, and harsher automated judgment.[50]

Biometric, Generative, And Surveillance – Driven Privacy Risks

Biometric and generative AI intensify privacy risks because they attach computation to the body, voice, face, gait, likeness, and personality. Surveillance expands when identification becomes persistent, remote, and automated across workplace, consumer, and public environments.[51]

7. CONCLUSION AND SUGGESTIONS

CONCLUSION:-

Artificial intelligence has made privacy a question of legal power rather than mere personal seclusion. The central anxiety is not only that intimate information may be exposed, but that ordinary data may be converted into prediction, classification, suspicion,

---

46 Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* 90 (New York University Press, New York, 1st edn., 2004).

47 AI, Data Governance and Privacy, *available at:* https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html (last visited on April 24, 2026).

48 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 202 (Profile Books, London, 1st edn., 2019).

49 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 67 (Harvard University Press, Cambridge, 1st edn., 2015).

50 Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* 85 (New York University Press, New York, 1st edn., 2018).

51 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 213 (PublicAffairs, New York, 1st edn., 2019).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

exclusion, or behavioural control. In that transformation, the individual becomes visible to systems that are often invisible to the individual. The study establishes that privacy in India cannot be understood as a recent statutory concern alone. Its intellectual foundations lie in older ideas of restraint, dignity, household boundaries, reputation, confidentiality, and limits on disclosure. Yet these foundations were historically uneven, because social status, gender, hierarchy, and community control shaped the reach of protection.

The historical inquiry shows that privacy moved gradually from moral restraint and domestic protection toward constitutional liberty and informational self-determination. Ancient and medieval legal cultures recognised protected spheres, but they did not produce an equal individual right. Colonial governance then converted communications into an object of administrative control, leaving privacy fragmented and subordinate to order.

The constitutional period supplied the decisive shift. Privacy became linked with liberty, dignity, autonomy, equality, and lawful restraint. This development is central to the study because AI does not merely invade space; it affects choice, identity, reputation, association, and access to opportunities through data-driven systems that often operate beyond ordinary public visibility. The study also finds that the DPDP Act's focus on personal data must be interpreted broadly in AI settings. Scraped, public, derived, inferred, or combined data may remain privacy-sensitive when linked to an identifiable person. The central issue is not the original appearance of the datum, but the capacity of aggregation and inference to alter its legal and social meaning.

Judicial development has been essential in preventing privacy from being frozen as a property-based or secrecy-based claim. The jurisprudential movement from bodily privacy and decisional autonomy to informational self-determination supplies the constitutional grammar for AI governance. Courts increasingly ask what consequences data systems produce, rather than relying only on the formal label attached to the data. It shows that proportionality, legality, necessity, safeguards, and contestability are indispensable when technologies affect privacy. This is especially important for biometric identity, communications surveillance, location tracking, automated scoring, and platform-based profiling. The legal inquiry must examine data acquisition, retention, inference, access, and downstream use together.

SUGGESTIONS

The following suggestions translate the study's findings into focused legal and policy measures that can strengthen privacy protection while permitting responsible AI development, especially in high-impact public, commercial, biometric, synthetic-media, and automated decision-making environments.

1. **Mandatory AI risk classification**: India should adopt a legally recognised classification of AI systems according to privacy and rights impact, with facial recognition, predictive policing, welfare eligibility, credit scoring, employment screening, health triage, and child-facing profiling treated as high-risk categories. This would align Indian governance with risk-based global practice without copying any foreign statute mechanically.
2. **AI impact assessment before deployment**: Every high-risk AI system should undergo an AI impact assessment covering personal data sources, purpose limitation, bias, security, explainability, human review, and foreseeable harm before deployment. The DPDP Rules already require annual data protection impact assessment for Significant Data Fiduciaries, and this mechanism should be expanded into an AI-specific assessment duty.
3. **Right to meaningful explanation:** Individuals affected by significant AI-assisted decisions should receive a meaningful explanation of the data categories used, the decision logic at an understandable level, and the responsible human authority. This is necessary because existing rights of access, correction, erasure, and grievance redressal are weak where the affected person cannot identify how the adverse outcome was produced.
4. **Human review for consequential decisions**: AI outputs that affect welfare, employment, education, credit, insurance, policing, health, or access to essential services should not become final without accessible human review. UNESCO's ethics framework treats human oversight, auditability, impact assessment, and due diligence as core safeguards, and India should convert these principles into enforceable sectoral duties.
5. **Public-sector AI procurement safeguards**: Government procurement of AI systems should require privacy-by-design clauses, data minimisation, explainability, audit access, security testing, error reporting, and vendor liability for unlawful processing. This is especially necessary because State deployment affects constitutional rights and because India's own responsible AI materials recognise the need for safe and responsible public-sector adoption.
6. **Biometric AI restriction framework:** Facial recognition, voice recognition, gait analysis, and other biometric AI tools should be permitted only under specific statutory authority, defined purpose, limited retention, independent approval, and post-deployment audit. Biometric identifiers cannot be replaced like passwords, so convenience-based deployment should not be allowed to mature into generalised identification infrastructure.
7. **Training-data provenance register:** Developers and deployers of high-risk AI systems should maintain a provenance register recording dataset sources, categories of personal data, scraping practices, licensing basis, de-identification measures, and removal mechanisms. This would directly address the gap between collection-time consent and later model training, where privacy harm often emerges after aggregation.
8. **Stronger notice for AI processing**: Notices under the DPDP Rules should expressly disclose when personal data will be used for model training, profiling, recommendation, automated scoring, or behavioural prediction. Rule 3 already requires clear, itemised, purpose-linked notice, and AI-specific disclosure would prevent vague purposes from authorising broad computational reuse.
9. **AI-specific security safeguards**: Data fiduciaries using AI should treat training datasets, embeddings, prompt histories, model logs, inference APIs, and fine-tuning data as protected processing environments. The DPDP Rules already require encryption, masking, access control, monitoring, logs, backups, and processor safeguards, and these should be expressly adapted to AI architectures.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

10. **AI breach and incident reporting**: CERT-In's cyber incident taxonomy should be operationalised for AI-specific incidents, including model inversion, training-data leakage, prompt injection causing exposure of personal data, data poisoning, adversarial compromise, and unauthorised model access. CERT-In's 2022 directions already recognise incidents affecting AI and machine-learning systems, making a more detailed reporting template the next necessary step.