THE CONSTITUTIONAL RIGHT TO PRIVACY IN INDIA AND CHALLENGES POSED BY ARTIFICIAL INTELLIGENCE

Priyanshu Mishra, Galgotias University

ABSTRACT

The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017) marked a constitutional milestone in Indian jurisprudence. However, the emergence of Artificial Intelligence (AI) has posed unprecedented challenges to this right, reshaping the relationship between individuals, the state, and private corporations. AI's reliance on big data, profiling, and predictive analytics threatens informational autonomy, decisional privacy, and human dignity. This article critically examines the evolution of privacy jurisprudence in India, the constitutional framework post-Puttaswamy, and the collision course between AI technologies and privacy rights. It draws comparative lessons from global regulatory models and identifies structural gaps in India's legal and institutional architecture. Finally, it proposes a roadmap for reforms—legislative, judicial, institutional, and cultural—to safeguard privacy in the AI age while fostering responsible innovation.

Keywords: Privacy, Constitution of India, Artificial Intelligence, Data Protection, Puttaswamy, Surveillance, Fundamental Rights, AI Governance

1. Introduction

Privacy, as a concept, is as old as human civilization, yet its legal recognition has been one of the most contested and evolving phenomena. In constitutional democracies, privacy is regarded as a safeguard against excessive state intrusion and a foundation for human dignity, liberty, and autonomy. For decades, privacy remained an ambiguous right within the Indian constitutional framework, largely dependent on fragmented judicial interpretations. However, in 2017, the Supreme Court in Justice K.S. Puttaswamy v. Union of India recognized the right to privacy as a fundamental right under Article 21 of the Constitution, heralding a new era of constitutionalism. This judgment elevated privacy from a peripheral claim to a core constitutional value.

While this recognition marked a significant milestone, the rapidly advancing landscape of digital technologies, particularly Artificial Intelligence (AI), has introduced challenges unforeseen by the framers of the Constitution or even the judiciary in Puttaswamy. AI systems, driven by the insatiable need for data, function by collecting, analyzing, and predicting patterns from vast amounts of personal and sensitive information. Although AI has the potential to revolutionize healthcare, education, governance, and economic growth, it also poses grave risks to informational privacy, autonomy, and even democratic institutions.

The tension between the constitutional right to privacy and the growing reliance on AI is evident in multiple domains. The state, in its quest for efficiency and security, increasingly deploys AI-based surveillance systems such as facial recognition technologies, predictive policing tools, and biometric databases. Private corporations, on the other hand, use AI-driven algorithms for profiling, targeted advertising, and consumer manipulation. In both contexts, individuals are often unaware of the extent to which their personal data is collected, processed, and repurposed, thereby raising questions about the validity of "informed consent." This asymmetry of power between the data subject and the data collector creates a situation where privacy risks are not only widespread but systemic.

The recognition of privacy as a constitutional right in Puttaswamy emphasized three dimensions—bodily, informational, and decisional privacy. Each of these dimensions is directly implicated in AI-driven technologies. Bodily privacy is threatened by biometric data collection (e.g., Aadhaar, DigiYatra). Informational privacy is endangered by large-scale data aggregation without transparency. Decisional privacy—the freedom to make choices without

manipulation—is undermined by algorithmic recommendations and micro-targeted political campaigns. The implications extend beyond individual rights to the functioning of democracy itself, as AI has the capacity to influence electoral outcomes, shape public opinion, and perpetuate structural inequalities.

Globally, different jurisdictions have attempted to address the AI-privacy dilemma through legal frameworks. The European Union has been a frontrunner with its General Data Protection Regulation (GDPR) and the recently enacted AI Act, both of which impose stringent obligations on data processing and AI governance. The United States, though lacking a federal privacy law, has adopted a sectoral approach, while China has adopted a highly state-controlled regulatory model that simultaneously enables and restricts AI use. India, however, is still at a nascent stage. The Digital Personal Data Protection Act, 2023, while a significant step forward, has been criticized for excessive exemptions granted to the state and for failing to address AI-specific risks such as algorithmic transparency and accountability.

The problem is not merely regulatory but also theoretical. Traditional legal frameworks were designed for human actors and human accountability. AI disrupts this by introducing machine-driven decision-making that is opaque, complex, and, at times, unpredictable. The question of who is accountable—developer, deployer, or the algorithm itself—remains unresolved in most jurisdictions, including India. Thus, the challenge is not only to expand privacy jurisprudence but also to rethink the very doctrines of accountability, consent, and proportionality in the age of AI.

Against this backdrop, this article seeks to examine the constitutional right to privacy in India and critically analyze the challenges posed by AI to this right. The article proceeds in the following structure:

1. **Historical Evolution of Privacy in India** – tracing its judicial journey from rejection in M.P. Sharma (1954) and Kharak Singh (1962) to recognition in Puttaswamy (2017).

2. Constitutional Framework Post-Puttaswamy – analyzing how privacy was conceptualized as a three-dimensional right and the judicial application of the proportionality test.

3. Artificial Intelligence and Privacy: Points of Conflict – exploring how AI technologies

such as facial recognition, algorithmic profiling, and data analytics infringe on bodily, informational, and decisional privacy.

4. Comparative Perspectives – examining global approaches, including the GDPR, EU AI Act, and the U.S. and Chinese models, to draw lessons for India.

5. Challenges in the Indian Context – highlighting gaps in India's legal and regulatory frameworks, particularly the limitations of the Digital Personal Data Protection Act, 2023.

6. Suggestions and Reforms – proposing a roadmap for AI regulation in India, including algorithmic transparency, accountability, and judicial oversight.

7. Conclusion – emphasizing the need to balance innovation with constitutional values.

The central thesis of this article is that while privacy has been constitutionally recognized as a fundamental right in India, the emergence of AI presents challenges that demand a recalibration of legal frameworks and judicial doctrines. The Constitution must be interpreted in a manner that safeguards individual rights in the digital age without stifling technological innovation. Only then can India strike the delicate balance between technological progress and constitutional morality.

2. Historical Evolution of Privacy in India

2.1 Early Judicial Rejections of Privacy

The recognition of privacy in Indian constitutional law has not been linear. In the early decades after independence, the Supreme Court of India took a narrow and textual approach to fundamental rights, emphasizing express provisions over implied guarantees. This interpretive methodology led to the rejection of privacy as a fundamental right in two landmark cases: M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1962).

In M.P. Sharma v. Satish Chandra, an eight-judge bench dealt with a challenge to search and seizure powers under the Code of Criminal Procedure in the context of corporate fraud investigations. The Court observed that the U.S. Constitution's Fourth Amendment explicitly guaranteed protection against unreasonable searches and seizures, whereas the Indian

Constitution contained no such parallel provision. The Court categorically held that the Indian Constitution did not recognize a general right to privacy, thus rejecting the claim. This textualist reasoning set the tone for the following decade, suggesting that privacy was alien to Indian constitutional design.

In Kharak Singh v. State of Uttar Pradesh, the issue was whether police surveillance practices, including domiciliary visits at night, violated fundamental rights. The majority struck down domiciliary visits as unconstitutional, but not on the ground of privacy; instead, the Court relied on the "personal liberty" component of Article 21. Importantly, the Court reiterated that the Constitution did not guarantee a fundamental right to privacy. Justice Subba Rao's dissent, however, marked a turning point. He argued that "personal liberty" in Article 21 was broad enough to include privacy, and that unauthorized intrusion into a person's home or private life was constitutionally impermissible. This dissent planted the seed for privacy's later acceptance.

These early decisions reflected the judiciary's reluctance to expand constitutional rights beyond explicit textual guarantees. The dominance of positivist interpretation, coupled with a strong emphasis on collective goals of the newly independent state, left little room for individual-centric rights such as privacy.

2.2 Gradual Acceptance and Expansion

The 1970s witnessed a shift in constitutional jurisprudence, driven by the expanding interpretation of Article 21 in cases such as Maneka Gandhi v. Union of India (1978). The Court began to read into Article 21 rights that were essential to dignity and liberty, even if not expressly mentioned. This broader interpretive method paved the way for privacy to be accepted as implicit in the Constitution.

In Gobind v. State of Madhya Pradesh (1975), the Court upheld police surveillance regulations but acknowledged that privacy, though not expressly guaranteed, could be read into Article 21. Justice Mathew observed that privacy was not an absolute right and must yield to compelling state interests. Importantly, the Court recognized privacy as essential to liberty and dignity, marking a doctrinal shift from M.P. Sharma and Kharak Singh.

Subsequent cases consolidated this position. In Malak Singh v. State of Punjab & Haryana (1981), the Court held that surveillance must not be arbitrary and should respect the dignity of

the individual. In R. Rajagopal v. State of Tamil Nadu (1994), popularly known as the "Auto Shankar case," the Court recognized the right of individuals to prevent unauthorized publication of their private lives. The Court linked privacy with freedom of expression, holding that unauthorized biographies and intrusive journalism violated privacy unless justified by public interest.

In People's Union for Civil Liberties (PUCL) v. Union of India (1997), the Court addressed telephone tapping under the Telegraph Act. The Court held that privacy was part of Article 21 and that telephone conversations were private communications protected from arbitrary interception. This case reinforced the informational aspect of privacy, anticipating challenges of the digital age.

These judgments demonstrated a gradual but unmistakable acceptance of privacy as a constitutional right, albeit implicit and subject to limitations. The Court began to recognize privacy as central to dignity, autonomy, and liberty.

2.3 Doctrinal Maturity and the Road to Puttaswamy

By the early 2000s, privacy had become a recognized but still unsettled right. Its scope and limitations remained undefined, and questions persisted about its constitutional foundation. The growing use of biometric databases, surveillance technologies, and the Aadhaar project intensified debates on privacy's status.

The Aadhaar scheme, launched in 2009, sought to provide unique identification numbers based on biometric and demographic data. Civil society groups challenged Aadhaar on the ground that it violated privacy. In response, the Union government argued that privacy was not a fundamental right, relying on the old precedents of M.P. Sharma and Kharak Singh. This forced the Supreme Court to reconsider the very existence of privacy as a fundamental right.

In Justice K.S. Puttaswamy v. Union of India (2017), a nine-judge Constitution Bench unanimously held that privacy is a fundamental right intrinsic to life and liberty under Article 21 and other fundamental rights. The judgment overruled M.P. Sharma and Kharak Singh, declaring privacy to be inalienable, natural, and central to human dignity.

The Court in Puttaswamy articulated privacy in three dimensions:

1. **Bodily Privacy** – protection against physical intrusions and unwanted access to the human body.

2. **Informational Privacy** – control over personal data and information in the digital age.

3. **Decisional Privacy –** autonomy in making intimate and personal choices.

Further, the Court emphasized that privacy is not absolute and can be restricted by a law that satisfies the test of legality, necessity, and proportionality. This proportionality test became the cornerstone of privacy jurisprudence, ensuring that restrictions are narrowly tailored and justified by legitimate state interests.

2.4 Privacy Beyond Puttaswamy: Expansion into Substantive Rights

Post-Puttaswamy, privacy has been invoked in multiple landmark cases. In Navtej Singh Johar v. Union of India (2018), decriminalizing same-sex relations, the Court explicitly linked privacy with decisional autonomy, emphasizing that intimate choices are shielded from state interference. Similarly, in Joseph Shine v. Union of India (2019), striking down adultery laws, the Court invoked privacy to protect individual choices in matters of intimacy.

The Aadhaar judgment (Puttaswamy II, 2018) refined the privacy framework by upholding Aadhaar's constitutionality but subjecting it to strict proportionality. While the scheme was retained, its use by private corporations was restricted, and stringent safeguards were mandated for data protection.

Through these developments, privacy matured into a substantive right that influences various domains—sexuality, family, data protection, freedom of expression, and even democracy. The Court positioned privacy as a core element of constitutional morality, ensuring that it evolves with changing societal and technological realities.

3. Constitutional Framework of Privacy Post-Puttaswamy

3.1 The Puttaswamy Judgment: A Watershed Moment

The decision in Justice K.S. Puttaswamy v. Union of India (2017) fundamentally altered the constitutional landscape of India. A nine-judge Constitution Bench unanimously held that the

right to privacy is a fundamental right, implicit in the guarantees of life and liberty under Article 21, and interwoven with the freedoms under Part III of the Constitution.

The judgment emphatically overruled M.P. Sharma and Kharak Singh, putting to rest decades of uncertainty. More importantly, it did not merely affirm privacy as a constitutional right but developed a comprehensive jurisprudential framework for its application.

3.2 The Three Dimensions of Privacy

The Court conceptualized privacy as comprising three overlapping but distinct dimensions:

1. **Bodily Privacy**
    - Concerns protection against physical intrusions, such as forced medical procedures, biometric data collection, or unauthorized searches.
    - Rooted in the autonomy of the individual over their own body.
2. **Informational Privacy**
    - Protects an individual's right to control the dissemination and use of personal data.
    - Especially relevant in the digital age where vast amounts of personal data are processed by the state and private actors.
3. **Decisional Privacy**
    - Protects the ability to make intimate personal decisions—such as marriage, procreation, sexuality, and faith—free from state interference.

This tripartite framework aligns with global privacy jurisprudence, particularly the U.S. focus on decisional autonomy and the European emphasis on informational privacy.

3.3 Doctrinal Tools: The Proportionality Test

The Court recognized that privacy is not absolute. To determine the validity of restrictions on privacy, it adopted the proportionality test, building on earlier precedents like Modern Dental

College v. State of Madhya Pradesh (2016). The test requires that:

1. **Legality –** There must be a law in existence to justify the restriction.
2. **Legitimate Aim –** The law must pursue a legitimate state interest.
3. **Necessity –** The measure must be necessary in a democratic society.
4. **Proportionality –** There must be a rational nexus between the restriction and the objective sought, and the measure must be the least restrictive alternative.

By embedding proportionality, the Court ensured that privacy restrictions must pass a rigorous constitutional threshold. This doctrine has since become central in adjudicating conflicts between privacy and state interests.

3.4 Privacy as Intrinsic to Dignity and Liberty

The judgment emphasized that privacy is intrinsic to the dignity of the individual. Justice Chandrachud, writing for the majority, observed:

"Privacy is the constitutional core of human dignity. Privacy ensures the fulfillment of dignity by enabling the individual to preserve the sanctity of personal intimacies, the autonomy of personal choices, and the control over dissemination of personal information."

This framing situates privacy not as a stand-alone right but as a value that underpins and enriches other rights—speech, equality, freedom of movement, and religion.

3.5 Post-Puttaswamy Applications

The Puttaswamy judgment did not exist in isolation; it quickly became the foundation for subsequent transformative rulings.

1. **Navtej Singh Johar v. Union of India (2018)**
    - Decriminalized same-sex relations under Section 377 of the IPC.
    - The Court linked sexual orientation with decisional privacy and autonomy, recognizing that intimate choices are shielded from majoritarian interference.

2. **Joseph Shine v. Union of India (2019)**
    - Struck down Section 497 IPC, which criminalized adultery.
    - The Court reasoned that the law intruded into the private sphere of marriage and decisional autonomy of individuals.
3. **Aadhaar (Puttaswamy II) (2018)**
    - A five-judge bench upheld the Aadhaar scheme but struck down provisions allowing private corporations to mandate Aadhaar.
    - The Court applied the proportionality test, holding that while Aadhaar served legitimate state interests (welfare distribution, identification), data use must be minimal and restricted to statutory purposes.

Through these rulings, privacy has been recognized not only as a fundamental right but also as a **transformative constitutional principle** that influences substantive areas of law.

3.6 Interaction with Other Fundamental Rights

Privacy's recognition also transformed the interpretation of other fundamental rights:

- **Article 14 (Equality)**: Algorithmic discrimination, profiling, and unequal treatment are now framed as violations of both equality and informational privacy.
- **Article 19 (Speech and Expression)**: Privacy ensures freedom of thought and expression without surveillance chilling democratic participation.
- **Article 25 (Freedom of Religion)**: Privacy protects the autonomy of belief and practice in personal faith.

This interrelationship confirms privacy's role as a **horizontal enabler** of the entire Part III framework.

3.7 Privacy and State Surveillance

One of the most significant contributions of Puttaswamy is the recognition that surveillance, if

unchecked, erodes democracy. The Court acknowledged that technological advancements had increased the potential for state intrusion. Informational privacy was specifically emphasized in this context, with the Court highlighting the risks of mass data collection.

The judgment's emphasis on proportionality thus serves as a constitutional check on emerging state practices like biometric databases, CCTV networks, and AI-driven predictive policing.

3.8 The Emerging Gap: Privacy and Artificial Intelligence

Despite its breadth, Puttaswamy was delivered in 2017, just as AI was beginning to gain mainstream traction. While it laid down general principles, it did not address AI-specific concerns such as:

- Algorithmic opacity ("black box" decision-making).
- Automated profiling and predictive analytics.
- Consent fatigue in data-driven systems.
- AI-driven manipulative practices such as deepfakes and targeted political campaigns.

Thus, while Puttaswamy provides the **doctrinal foundation**, it requires expansion and adaptation to meet the challenges posed by AI. The proportionality test may serve as a constitutional safeguard, but its application to opaque algorithms and machine learning systems remains untested in Indian courts.

4. AI and Privacy: The Collision Course

4.1 Introduction: AI's Transformative but Intrusive Potential

Artificial Intelligence (AI) has emerged as one of the most transformative technologies of the 21st century. By enabling machines to perform tasks that require human-like intelligence—such as decision-making, natural language processing, and predictive analytics—AI has revolutionized healthcare, finance, education, governance, and security. At the same time, AI has introduced **unprecedented risks to privacy**, particularly in a jurisdiction like India where data protection laws are still nascent.

AI's power lies in its ability to **collect, process, and analyze massive datasets**, often including personal and sensitive information. Machine learning algorithms thrive on patterns extracted from individuals' behaviors, preferences, biometrics, and communications. While this enables efficiency and innovation, it also leads to profiling, surveillance, and manipulation at scales previously unimaginable.

This dual nature of AI—progressive yet invasive—creates a direct collision course with the constitutional right to privacy recognized in Puttaswamy.

4.2 AI and Bodily Privacy

Bodily privacy, as recognized in Puttaswamy, protects individuals from physical intrusions and unauthorized access to the human body. AI technologies increasingly blur the boundaries of bodily integrity:

1. **Biometric Surveillance**
    - AI-driven facial recognition systems (FRS) are being deployed by law enforcement agencies in India, such as during protests (e.g., anti-CAA demonstrations).
    - These systems capture and analyze unique biometric identifiers without consent, raising concerns of "function creep" where data collected for one purpose is repurposed for surveillance.
    - Bodily privacy is compromised as individuals are identified and tracked in public spaces without their knowledge.
2. **Healthcare AI and Genetic Data**
    - AI tools in healthcare rely on large datasets, including genetic information and medical records.
    - While they promise personalized treatment, they also create risks of misuse, discrimination (e.g., denial of insurance), or breaches.
    - The absence of robust anonymization mechanisms exacerbates these concerns.

3. **Wearable Devices and Internet of Bodies (IoB)**

    - Fitness trackers, smartwatches, and IoT-enabled medical devices continuously collect physiological data.
    - When processed by AI, these data points reveal intimate details about an individual's health, lifestyle, and even emotional states.
    - Such intrusions erode the "bodily autonomy" emphasized in Puttaswamy.

Thus, AI challenges the sanctity of bodily privacy by transforming the human body into a **data-generating object**, subject to constant observation and commodification.

4.3 AI and Informational Privacy

Informational privacy lies at the heart of AI-related concerns. AI thrives on **big data ecosystems**, where personal information becomes raw material for algorithms.

1. **Data Harvesting and Profiling**

    - Social media platforms, search engines, and e-commerce companies use AI to track users' behavior, preferences, and interactions.
    - AI builds "digital dossiers" that reveal far more than individuals willingly disclose.
    - For instance, targeted advertising systems can infer political leanings, sexual orientation, or mental health conditions based on online activity.

2. **Algorithmic Decision-Making**

    - Credit scoring, hiring platforms, and predictive policing increasingly rely on AI.
    - These systems use personal data to make consequential decisions without transparency.
    - Errors or biases in training data can lead to discrimination, undermining both privacy and equality under Article 14.

3. **Opacity of AI Systems**
    - AI often operates as a "black box," where neither users nor regulators fully understand how decisions are made.
    - This opacity undermines accountability and makes it nearly impossible for individuals to exercise control over their personal data.
4. **Cross-Border Data Flows**
    - AI platforms are often global, involving transfer of data to jurisdictions with weaker safeguards.
    - India's legal framework for cross-border data transfer remains underdeveloped, leaving informational privacy vulnerable.

In essence, AI transforms personal data into a **commodity**, undermining the control individuals have over their own information.

4.4 AI and Decisional Privacy

Decisional privacy ensures autonomy in making intimate and personal choices. AI challenges this by subtly influencing—or outright manipulating—decision-making:

1. **Behavioral Targeting and Manipulation**
    - Platforms like Facebook and YouTube use AI algorithms to maximize engagement by recommending personalized content.
    - This can create "filter bubbles" and "echo chambers," limiting exposure to diverse viewpoints and subtly steering political opinions.
    - The Cambridge Analytica scandal demonstrated how AI-driven microtargeting could manipulate democratic choices.
2. **Deepfakes and Synthetic Media**
    - AI tools generate hyper-realistic fake videos or audios (deepfakes), which can

distort reality and harm reputations.

- Deepfakes also pose risks of non-consensual pornography, blackmail, and political misinformation—direct assaults on decisional autonomy.

3. **Predictive Analytics and Nudging**

- AI can predict individual preferences with high accuracy and use this to nudge behaviors (e.g., consumer purchases, voting patterns).

- While framed as personalization, such nudging compromises the individual's ability to make free and independent choices.

Thus, AI intrudes into the **inner forum of decision-making**, where privacy is most essential. It undermines autonomy by replacing free will with algorithmically guided preferences.

4.5 Case Studies: AI and Privacy in India

1. **Facial Recognition in Policing**

- Delhi Police reportedly used FRS to identify individuals during public protests.

- The lack of statutory safeguards or judicial oversight highlights the dangers of AI-enabled surveillance in eroding privacy.

2. **Aadhaar Ecosystem and AI**

- While not an AI system per se, Aadhaar's biometric database serves as a foundation for AI-driven analytics.

- Linking Aadhaar with welfare schemes, telecom services, and banking creates a massive centralized database vulnerable to misuse.

3. **EdTech Platforms**

- During the COVID-19 pandemic, educational platforms used AI to monitor student engagement, including facial expressions and keystroke patterns.

- Such practices intruded into both informational and decisional privacy of minors without adequate safeguards.

These examples underscore how AI applications, even when designed for public interest, often operate in a regulatory vacuum with profound privacy consequences.

4.6 AI and the State: The Threat of Surveillance Capitalism

The risks posed by AI are magnified in contexts where the state becomes both regulator and user of technology.

- **Mass Surveillance**: AI enables the state to implement predictive policing, social credit systems, and population-scale monitoring.
- **National Security Justifications**: The state often invokes security concerns to justify intrusive AI systems, undermining the proportionality test laid down in Puttaswamy.
- **Chilling Effect on Democracy**: Continuous surveillance discourages dissent and free expression, eroding democratic participation.

This convergence of state power and AI technology risks creating what scholars call a "surveillance state," where privacy ceases to be meaningful.

4.7 Gaps in the Constitutional Framework

While Puttaswamy provides a doctrinal foundation, several gaps remain when applied to AI:

1. **Opacity vs. Proportionality**
    - The proportionality test requires evaluating necessity and minimal intrusion. But how can courts assess proportionality when AI algorithms are opaque and not explainable?
2. **Consent Fatigue**
    - Current privacy protection relies on user consent. In AI ecosystems, consent becomes meaningless when individuals cannot comprehend how data will be used.

3. **Private vs. State Intrusions**

    - The Constitution primarily addresses state action. Yet, in AI-driven economies, private corporations pose equally serious threats to privacy. Puttaswamy left open the question of horizontal application of privacy rights.

4. **Lack of Institutional Capacity**

    - Indian courts and regulators often lack technical expertise to scrutinize AI systems, leaving enforcement weak.

5. Comparative Perspectives on Privacy and AI

5.1 Introduction: Why Comparative Perspectives Matter

Constitutional rights do not evolve in isolation. Privacy, in particular, has been shaped by global dialogues across jurisdictions. In an interconnected digital economy, where AI systems are often developed in one country, trained on data from another, and deployed worldwide, **national privacy frameworks must engage with international standards**.

India's Puttaswamy judgment already drew upon comparative jurisprudence—from the U.S. right to decisional autonomy to the European emphasis on data protection. In the AI era, comparative perspectives are even more essential, as they provide tested regulatory tools and highlight pitfalls to avoid.

5.2 The European Union: GDPR and the AI Act

The European Union (EU) represents the most advanced privacy framework globally, characterized by strong individual rights and robust regulatory mechanisms.

5.2.1 General Data Protection Regulation (GDPR)

Enforced in 2018, the GDPR is widely regarded as the gold standard in data protection. Its relevance to AI and privacy lies in several key principles:

1. **Lawfulness, Fairness, and Transparency**

- Data processing must have a lawful basis (consent, contract, legitimate interest).
- Individuals must be informed of how their data is collected and used.
- AI systems using personal data must be transparent.

2. **Data Minimization and Purpose Limitation**
   - AI systems cannot collect more data than necessary or repurpose it beyond the initial purpose without consent.
3. **Rights of Individuals**
   - **Right to Access and Rectification**: Users can know and correct data about them.
   - **Right to Erasure ("Right to be Forgotten")**: Individuals can demand deletion of their data.
   - **Right to Data Portability**: Users can transfer their data between service providers.
   - **Right to Object to Automated Decision-Making**: Article 22 GDPR gives individuals the right not to be subjected to decisions based solely on automated processing, including profiling, if such decisions have legal or significant effects.
4. **Accountability and Data Protection Impact Assessments (DPIA)**
   - AI systems with high privacy risks must undergo impact assessments before deployment.

The GDPR thus provides a **direct framework for regulating AI**, especially in contexts like profiling and algorithmic decision-making.

5.2.2 The Proposed EU Artificial Intelligence Act (AI Act)

Recognizing that GDPR alone is insufficient, the EU has proposed the **AI Act**, the first

comprehensive law specifically regulating AI. Its approach is risk-based:

1. **Unacceptable Risk AI** – Completely banned (e.g., social scoring, manipulative AI, certain real-time facial recognition).

2. **High-Risk AI** – Allowed but subject to strict obligations (e.g., medical AI, recruitment algorithms, credit scoring). Requirements include transparency, human oversight, and accuracy.

3. **Limited-Risk AI** – Subject to minimal transparency requirements (e.g., chatbots must disclose they are AI).

4. **Minimal Risk AI** – Freely permitted (e.g., video games using AI).

The AI Act complements GDPR by addressing **algorithmic opacity**, **bias**, and **human oversight**, directly targeting AI's challenges to privacy and autonomy.

5.3 United States: Sectoral Approach and Free Speech Concerns

The United States lacks a single comprehensive data protection law. Instead, it follows a **sectoral approach**, where specific industries (healthcare, finance, children's data) are regulated by separate statutes.

5.3.1 Key Privacy Regulations

1. **Health Insurance Portability and Accountability Act (HIPAA)** – Protects health data.

2. **Children's Online Privacy Protection Act (COPPA)** – Regulates online collection of children's data.

3. **California Consumer Privacy Act (CCPA)** – State-level law providing GDPR-like rights, including data access and deletion.

This fragmented approach means that AI companies often face fewer constraints compared to Europe.

5.3.2 AI and Constitutional Concerns

- The U.S. Constitution does not explicitly recognize privacy, but courts have read it into the Fourth Amendment (protection against unreasonable searches) and the Fourteenth Amendment (decisional autonomy).

- However, the strong protection of **free speech under the First Amendment** complicates regulation of AI-driven targeted advertising and misinformation. Courts often strike down restrictions on data use as violations of free speech.

The U.S. approach illustrates a trade-off: it fosters innovation but often at the cost of weak privacy protections. Scandals such as Cambridge Analytica reveal the dangers of under-regulation.

5.4 United Kingdom: Post-Brexit Privacy Framework

After Brexit, the U.K. retained GDPR principles through the **Data Protection Act 2018**, but has shown interest in diverging for greater regulatory flexibility.

- The U.K. Information Commissioner's Office (ICO) has issued guidance on **AI auditing frameworks**, emphasizing fairness, transparency, and accountability.

- The U.K. has also adopted a **"pro-innovation" regulatory approach**, promoting AI development while stressing "explainability" in automated decision-making.

This balance between innovation and privacy is delicate, and critics argue that weakening GDPR standards could erode individual rights.

5.5 Canada: Rights-Based Data Protection and AI Regulation

Canada's privacy framework is rooted in the **Personal Information Protection and Electronic Documents Act (PIPEDA)**, which governs private-sector data practices.

- Canada is currently considering the **Artificial Intelligence and Data Act (AIDA)**, which would regulate high-impact AI systems, emphasizing transparency and accountability.

- Canadian privacy regulators have been vocal in linking AI to constitutional values, stressing that automated decision-making must respect dignity and equality.

Canada's rights-based but pragmatic approach resonates closely with India's constitutional ethos.

5.6 China: State-Centric Approach to AI and Privacy

China provides a starkly different model. While it has enacted the **Personal Information Protection Law (PIPL)** and **Data Security Law**, these frameworks prioritize **state interests** over individual rights.

- AI is extensively used in state surveillance, including the infamous **social credit system** and facial recognition for monitoring ethnic minorities.

- While private corporations are somewhat regulated, the state itself is largely exempt from meaningful privacy obligations.

China demonstrates how AI can entrench authoritarian governance, eroding decisional autonomy and informational privacy on a mass scale. For India, this model serves as a cautionary tale of what to avoid.

5.7 International Human Rights Instruments

Global instruments also shape AI and privacy discourse:

1. **Universal Declaration of Human Rights (UDHR), 1948 – Article 12**: Protects individuals from arbitrary interference with privacy.

2. **International Covenant on Civil and Political Rights (ICCPR), 1966 – Article 17**: Expands on privacy protections, binding on state parties, including India.

3. **OECD AI Principles (2019)**: Emphasize human-centered values, transparency, and accountability.

4. **UNESCO's AI Ethics Recommendation (2021)**: Calls for AI governance rooted in human rights, fairness, and sustainability.

India, as a signatory to many of these instruments, has both an obligation and an opportunity to align domestic privacy jurisprudence with global norms.

5.8 Lessons for India

From these comparative perspectives, several key lessons emerge:

1. **Adopt Comprehensive Legislation**
    - Like GDPR, India must adopt a single, comprehensive law governing both data protection and AI, rather than fragmented rules.
2. **Risk-Based Regulation**
    - The EU AI Act's categorization of risks offers a model for regulating AI without stifling innovation.
3. **Transparency and Explainability**
    - Borrowing from the U.K. and Canada, India must mandate explainability in AI decision-making to make the proportionality test meaningful.
4. **Guard Against Surveillance Overreach**
    - China's example warns of state-centric misuse. India must ensure independent oversight to prevent AI from becoming a tool of authoritarianism.
5. **Ensure Horizontal Application of Privacy**
    - U.S. experience with corporate data exploitation shows the need to extend privacy protections to private actors, not just the state.

6. Challenges in the Indian Legal Landscape

6.1 Introduction

While Puttaswamy laid down a robust constitutional foundation for privacy, the **translation of this doctrine into practice** remains fraught with challenges. India stands at a critical juncture:

AI technologies are being rapidly deployed by both the state and private actors, yet the institutional, legislative, and regulatory ecosystem remains underdeveloped. This creates a dangerous gap where constitutional promises of privacy exist largely in theory, while on the ground, violations are rampant and unaddressed.

6.2 Fragmented Legislative Framework

India does not yet have a **comprehensive privacy law** equivalent to the EU's GDPR.

- The **Information Technology Act, 2000 (IT Act)** and its rules provide limited protections, focusing mainly on cybersecurity and data breaches.
- The **Digital Personal Data Protection Act, 2023 (DPDPA)**, recently enacted, is a step forward but falls short of international standards. It lacks:
    - Strong rights such as data portability or the right to object to automated decisions.
    - Independent oversight; the Data Protection Board is appointed by the government, raising concerns of executive control.
    - Clear obligations on AI-specific risks like profiling, algorithmic bias, and explainability.

This fragmented framework makes it difficult to regulate AI-driven intrusions into privacy.

6.3 Weak Institutional Capacity

Even where laws exist, **enforcement mechanisms are weak**:

- **Regulatory Agencies**: The proposed Data Protection Board lacks autonomy and technical expertise.
- **Judiciary**: Courts have constitutional authority but often lack the technical capacity to scrutinize complex AI algorithms. Judicial delay further compounds the problem.
- **Civil Society**: While active in advocacy, civil society organizations face challenges in accessing information due to the opacity of AI systems and lack of mandatory

transparency obligations.

The absence of specialized institutions for AI oversight leaves privacy protection largely aspirational.

6.4 State-Centric Intrusions

One of the most pressing challenges is the **state's own role as a violator of privacy**.

1. **Mass Surveillance Projects**
    - The **Central Monitoring System (CMS)** and **NATGRID** allow bulk interception of communications without judicial oversight.
    - AI-powered facial recognition is being deployed by police and government departments without a statutory framework.
2. **Aadhaar Ecosystem**
    - While upheld by the Supreme Court, Aadhaar continues to raise concerns of data misuse and excessive linkage with services.
    - The ecosystem creates the risk of centralized databases vulnerable to hacking and unauthorized surveillance.
3. **National Security Justifications**
    - The government frequently invokes national security to justify privacy-intrusive practices. However, the lack of proportionality analysis or independent review makes these claims difficult to challenge.

This creates a paradox: the very state tasked with protecting privacy often becomes its biggest threat.

6.5 Private Sector Dominance

The private sector, particularly **Big Tech companies**, poses equal if not greater risks:

- **Data Exploitation**: Social media, e-commerce, and fintech platforms collect massive amounts of personal data, often without meaningful consent.
- **Algorithmic Opacity**: AI-driven decisions in hiring, lending, and healthcare remain unexplainable, leaving individuals with no recourse.
- **Weak Liability Mechanisms**: Indian law lacks strong accountability requirements for private corporations deploying AI.

Without extending privacy rights **horizontally** against private actors, constitutional protections remain incomplete.

6.6 Cultural and Social Challenges

Privacy as a constitutional value often collides with **socio-cultural realities**:

- In a collectivist society like India, privacy is sometimes perceived as secondary to family, community, or state interests.
- Lack of awareness means individuals often undervalue or unknowingly trade away their privacy rights (e.g., accepting app permissions without scrutiny).
- In rural and marginalized communities, the harms of AI-driven exclusion (e.g., denial of welfare due to biometric mismatch) are particularly severe.

These challenges show that privacy must be contextualized within India's socio-economic fabric, not merely transplanted from Western models.

6.7 Judicial Inertia Post-Puttaswamy

Although Puttaswamy was transformative, its momentum has slowed:

- Courts have yet to develop detailed doctrines applying proportionality to AI-driven intrusions.
- There is limited jurisprudence on private sector violations.
- Ongoing cases, such as those concerning Pegasus spyware, highlight judicial reluctance

to confront the state directly on surveillance issues.

This judicial inertia risks reducing Puttaswamy to symbolic value rather than an enforceable safeguard.

7. Suggestions and Law Reform Proposals

7.1 Introduction

The challenges identified in the previous section reveal a significant **implementation gap** between constitutional recognition of privacy and the realities of the AI age. To bridge this gap, India must adopt a **multi-pronged reform strategy**, combining legal, institutional, and societal measures. This section sets out key proposals that can guide policymakers, courts, and civil society in building a privacy framework that is both constitutionally sound and technologically resilient.

7.2 Strengthening the Data Protection Regime

The **Digital Personal Data Protection Act, 2023 (DPDPA)** is a milestone but needs substantial improvement:

1. **Expand Data Subject Rights**
    - Introduce the **right to data portability**, **right to object to profiling**, and **right against fully automated decisions**, similar to the GDPR.
    - Recognize a **right to explanation** in AI contexts, requiring companies to provide intelligible reasons for algorithmic outcomes.
2. **Limit State Exemptions**
    - Narrow the broad government exemptions currently allowed under the DPDPA.
    - Require **judicial or independent approval** for data processing justified on national security grounds.
3. **Independent Regulatory Authority**
    - Replace the government-controlled Data Protection Board with a **truly**

independent Data Protection Authority.

- Ensure it has expertise in AI, cybersecurity, and human rights law.

By strengthening these areas, the DPDPA can evolve into a genuine safeguard against AI-driven privacy violations.

7.3 Enacting AI-Specific Legislation

While the DPDPA focuses on personal data, AI raises unique challenges that demand **dedicated legislation**.

- **Algorithmic Accountability Act**: A statute requiring companies to conduct **Algorithmic Impact Assessments (AIAs)** before deploying high-risk AI.
- **Transparency Obligations**: Mandating disclosure of datasets, training methods, and decision-making logic, subject to trade-secret protections.
- **Bias Audits**: Independent audits to detect and mitigate algorithmic discrimination in lending, hiring, healthcare, and policing.
- **Sandbox Approach**: Allow regulators to test AI applications in controlled environments before mass deployment.

Such legislation would complement existing data protection laws and provide clarity for industry while protecting citizens.

7.4 Judicial Innovations: Towards Algorithmic Due Process

The Indian judiciary has historically played a transformative role in expanding fundamental rights. It must now adapt privacy jurisprudence to the AI age.

1. **Developing Algorithmic Due Process**
    - Courts should extend principles of **natural justice** to AI-driven decisions, ensuring the right to notice, explanation, and appeal.
    - This aligns with the constitutional commitment to fairness under **Article 14**

(equality before law).

2. **Proportionality in AI Surveillance**
    - The proportionality test from *Puttaswamy* should be explicitly applied to AI-enabled surveillance systems.
    - Surveillance must be lawful, necessary, proportionate, and subject to independent oversight.
3. **Horizontal Application of Rights**
    - Courts should recognize the **horizontal application** of privacy rights, holding private corporations accountable for intrusions.
    - This mirrors jurisprudence in South Africa and the EU, where fundamental rights extend beyond state action.

Judicial innovations can thus fill gaps until comprehensive legislation is enacted.

7.5 Building Institutional Capacity

Institutions are crucial to operationalizing privacy guarantees. India must:

- **Establish a National AI Regulatory Authority**
    - Modeled on the EU's proposed AI Office, it would oversee AI deployment, certify high-risk systems, and impose penalties.
- **Enhance Technical Expertise of Judiciary**
    - Judicial academies should introduce training on AI, big data, and privacy law.
    - Courts may consider appointing **amicus curiae or technical experts** in AI-related cases.
- **Empower Data Protection Authority**
    - Give it investigatory powers, financial autonomy, and capacity to coordinate

with global regulators.

Without institutional strength, even the best laws will remain on paper.

7.6 Ethical AI Frameworks and Industry Standards

Beyond legal mandates, **self-regulation and ethical commitments** by industry can play a significant role:

- **Principles for Responsible AI**
    - Fairness, transparency, accountability, non-discrimination, and respect for human dignity.
- **Corporate Governance Reforms**
    - Boards of tech companies should include **AI ethics committees**.
    - Mandatory **environmental, social, and governance (ESG) disclosures** should include privacy and AI practices.
- **Certification and Labelling**
    - "Privacy by Design" certification can help consumers identify trustworthy products.

These frameworks can create a **culture of accountability** that goes beyond compliance.

7.7 Enhancing Public Awareness and Digital Literacy

Legal and institutional reforms will fail without citizen engagement. Steps include:

- **Curriculum Integration**: Introduce digital privacy modules in schools and universities.
- **Mass Awareness Campaigns**: Use television, radio, and social media to educate citizens about privacy rights and AI risks.

- **Civil Society Empowerment**: Strengthen NGOs and academic institutions working on digital rights, enabling them to monitor AI deployments and litigate violations.

Public participation is essential to ensure that privacy becomes a lived reality, not an abstract principle.

7.8 Comparative Lessons for India

India can learn from global approaches while tailoring them to its unique context:

- **From the EU**: Strong data subject rights and independent regulators.
- **From the US**: Sector-specific rules with flexibility for innovation.
- **From China**: The risks of unchecked state power in AI deployment, which India must avoid.
- **From Brazil's LGPD**: A hybrid model balancing rights with innovation.

Adopting a **"middle path"**, India should combine EU-style rights with US-style innovation incentives, while resisting authoritarian tendencies.

7.9 Summary of Recommendations

1. **Strengthen the DPDPA** with expanded rights, narrow exemptions, and independent oversight.
2. **Enact AI-specific legislation** on accountability, transparency, and bias audits.
3. **Develop judicial doctrines** of algorithmic due process and proportionality.
4. **Build institutional capacity** through specialized regulators and judicial training.
5. **Promote ethical AI practices** via corporate governance reforms.
6. **Enhance public awareness** to empower individuals against privacy intrusions.
7. **Draw comparative lessons** while contextualizing reforms to Indian realities.

8. Conclusion

8.1 Reaffirming Privacy as a Constitutional Bedrock

The recognition of privacy as a **fundamental right in Justice K.S. Puttaswamy v. Union of India (2017)** was not merely a judicial pronouncement—it was a constitutional milestone affirming the centrality of human dignity, autonomy, and liberty in the Indian democratic framework. Yet, the advent of **Artificial Intelligence (AI)** has complicated this achievement. The very technologies that promise efficiency, innovation, and growth also generate unprecedented risks of surveillance, profiling, manipulation, and exclusion.

8.2 A Constitutional-Technology Tension

The **constitutional promise of privacy** collides with the **technological logic of AI**, which thrives on mass data collection and predictive analytics. This tension has exposed structural weaknesses in India's privacy regime: fragmented laws, weak institutions, overbroad state powers, and limited judicial engagement. Without urgent reforms, there is a real danger that privacy will remain a **paper right**, eroded silently by digital practices that outpace legal oversight.

8.3 The Imperative of Reform

The way forward requires a **holistic strategy**:

1. **Legislative Reforms** → Strengthen the **Digital Personal Data Protection Act, 2023**, and enact **AI-specific legislation** ensuring accountability, transparency, and fairness.

2. **Judicial Innovation** → Courts must develop doctrines of **algorithmic due process** and apply the **proportionality test** rigorously to AI-driven intrusions.

3. **Institutional Capacity** → Establish independent regulators with technical expertise and autonomy.

4. **Cultural Change** → Promote digital literacy and empower citizens to assert their privacy rights.

5. **Global Alignment** → Learn from the EU, US, and other jurisdictions while tailoring

solutions to India's democratic ethos and developmental needs.

8.4 Balancing Innovation and Rights

India's ambition to become a global leader in AI cannot come at the cost of fundamental rights. The choice is not between **innovation** and **privacy**, but in finding a constitutional equilibrium that safeguards both. A strong privacy framework can in fact enhance trust in AI systems, encourage responsible innovation, and strengthen India's position in the global digital economy.

8.5 Closing Reflection

The **constitutional right to privacy** in India is both a shield and a compass: a shield against intrusive technologies, and a compass guiding the ethical development of AI. The challenge is immense, but so too is the opportunity. If India can successfully embed privacy into its AI governance framework, it will not only protect its citizens but also offer a model to the world of how constitutional democracies can thrive in the digital age.

In the final analysis, the question is not whether privacy can survive the rise of AI—it must. The deeper challenge is whether **India's institutions, laws, and citizens** can rise to the occasion. The answer to that challenge will shape the contours of Indian democracy in the 21st century.

References

- Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
- State of West Bengal v. Anwar Ali Sarkar, AIR 1952 SC 75.
- M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
- Kharak Singh v. State of U.P., AIR 1963 SC 1295.
- Gobind v. State of M.P., AIR 1975 SC 1378.
- R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
- PUCL v. Union of India, (1997) 1 SCC 301.
- Digital Personal Data Protection Act, 2023 (India).
- Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
- Solove, D.J., Understanding Privacy (Harvard University Press, 2008).
- Narayan, A., "The Right to Privacy in India: Constitutional and Common Law Perspectives," (2019) 12 NUJS L Rev 101.
- Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).
- California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–199 (2018).
- Personal Information Protection Law (PIPL) of China, 2021.
- Lei Geral de Proteção de Dados (LGPD), Law No. 13,709 of 2018 (Brazil).