International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 09 Issue 02 February 2026

DOI: 10.47191/ijsshr/v9-i2-32, Impact factor- 8.007

Page No: 1144-1162

Privacy and Data Protection in AI: A Comparative Analysis of EU and Indian Regulatory Frameworks

Tushita Gupta[1], Dr. Vivek Junghare[2]

[1]Independent Researcher

[2]Post-Doctoral Fellow, Uppsala University, Sweden

ABSTRACT: The rapid proliferation of artificial intelligence (AI) technologies has fundamentally transformed how personal data is collected, processed, and utilized across global jurisdictions. As AI systems increasingly permeate critical sectors—from healthcare and finance to law enforcement and social services—the tension between technological innovation and fundamental privacy rights has intensified. This paper examines the regulatory approaches to privacy and data protection in AI, with particular emphasis on comparing the European Union's General Data Protection Regulation (GDPR) framework with India's evolving data protection regime, specifically the Digital Personal Data Protection Act (DPDP) of 2023.

The comparative analysis focuses on three critical dimensions: (1) AI surveillance and the right to privacy, (2) consent and data ownership in machine learning systems, and (3) biometric data regulation and facial recognition technologies. These areas represent the frontier of regulatory challenges where the capabilities of AI systems most directly confront individual privacy rights and societal values. While the EU has established a comprehensive, rights-based framework through the GDPR, India's regulatory landscape reflects a hybrid approach that balances data protection principles with developmental priorities and state interests.

Understanding these divergent yet converging regulatory philosophies is essential for multinational organizations, policymakers, and researchers navigating the complex terrain of AI governance. The adequacy of cross-border data flows, enforcement mechanisms, and practical implementation challenges all hinge on how these jurisdictions operationalize their respective frameworks in the context of rapidly evolving AI capabilities.

1. INTRODUCTION

The significance of this research is underscored by AI's pervasive role in governance, healthcare, finance, and justice, with global AI investments projected to reach billions, necessitating robust regulation to balance innovation with ethical safeguards (Bose, 2025). Since the resurgence of AI research post-2010, the field has evolved rapidly, with increasing attention to ethical, legal, and social implications. The societal significance is underscored by the widespread adoption of AI systems, with over 85% of financial institutions employing AI technologies (Chopra, 2024), and legislative efforts like the EU AI Act and the US Algorithmic Accountability Act aiming to regulate AI usage. In order to preserve public confidence and protect fundamental rights, it is imperative that AI systems function in a transparent, equitable, and accountable manner.

Despite these advances, significant regulatory gaps persist, particularly in emerging economies like India, where AI-specific legislation remains fragmented or absent (Basu & Dave, 2025). While the EU has adopted a unified, risk-based regulatory approach emphasizing human rights and transparency, India relies on sector- specific policies and general laws such as the Information Technology Act, 2000, which inadequately address AI's unique challenges (Singh & Arora, 2025). This disparity has sparked debate over the adequacy of existing frameworks, with some advocating for comprehensive AI laws to mitigate risks like algorithmic bias, data misuse, and accountability deficits, while others caution against stifling innovation through overregulation (Cornelius, 2025).

These gaps have serious repercussions, such as the continuation of discrimination, deterioration of democratic values, potential market disruptions, ethical violations, erosion of public trust in AI systems, and a decline in the general well-being of society (Finch & Butt, 2025). In order to facilitate meaningful oversight and user comprehension, the critical knowledge gap in the effective operationalisation of transparency and explainability has to be addressed.

2. LITERATURE REVIEW

The literature highlights widespread problems of systemic bias and opacity by examining AI bias, algorithm transparency, and decision-making procedures. It identifies gaps in current legal frameworks and ethical guidelines that hinder effective accountability. The findings underscore the necessity for stronger regulatory policies to ensure equitable AI practices and informed governance.

2.1 Introduction

The key concepts of algorithmic transparency, bias mitigation, and accountability within AI governance are integrated into the conceptual framework that directs this review. To allow for scrutiny and trust, transparency entails explaining AI decision-making procedures to stakeholders; to maintain fairness and non-discrimination, bias—a term used to describe systematic unfairness ingrained in AI systems—needs to be identified and mitigated; accountability encompasses mechanisms to assign responsibility for AI outcomes, including legal and ethical dimensions (Cheong, 2024). These interrelated concepts form the foundation for evaluating AI governance frameworks and assisting policy development.

This study aims to bridge the gap between abstract ethical principles and practical regulatory mechanisms to offer actionable insights for stakeholders engaged in AI governance and contribute to advancing responsible AI deployment that aligns with societal values and human rights.

2.2 Statement of Purpose

The objective of this report is to examine the existing research to provide a comprehensive understanding of how contemporary legal and ethical paradigms are being reshaped by artificial intelligence technologies. This review is important as it seeks to identify gaps and strengths within current regulatory approaches, particularly contrasting the mature, risk-based framework of the European Union with the evolving and fragmented regulatory landscape in India. By synthesizing global perspectives alongside detailed jurisdictional analyses, the report aims to inform policymakers, legal scholars, and technologists about the adequacy of existing frameworks in addressing AI's multifaceted challenges, thereby guiding future regulatory development that balances innovation with ethical governance.

2.3 Thematic Review of Literature

Theme	Theme Description
Comparative Analysis of AI Regulatory Frameworks in EU and India	Most literature contrasts the EU's pioneering, comprehensive, and risk- based AI regulatory framework with India's fragmented and nascent AI governance. The EU AI Act emphasizes strong safeguards for fundamental rights, transparency, and enforceability, while Indian regulation lacks dedicated AI laws, relying on sectoral and policy frameworks, creating gaps in accountability and oversight (Basu & Dave, 2025). This comparative approach highlights India's urgent need for legislative innovation guided by international best practices.
Ethical and Human Rights Considerations in AI Governance	Ethical challenges such as algorithmic bias, privacy, transparency, and human dignity form the core concerns in AI regulation. The EU's human rights-based regulatory approach integrates constitutional protections with AI governance, whereas India's ethical AI frameworks remain largely emergent and fragmented. Scholars emphasize embedding ethics into law and policy, advocating for human rights- centric models to prevent 'ethics washing' and ensure accountability (Olariu & Zeleznikow, 2025). Ethical principles are increasingly operationalized in regulations but vary in enforceability and scope.
Risk-based and Standards-driven Regulatory Approaches	The EU's AI Act exemplifies a risk-tiered framework categorizing AI systems by risk levels with corresponding obligations, supported by ISO standards and ethical benchmarks. This approach balances innovation with precaution, aiming to mitigate harms from high-risk AI applications. Studies critique challenges such as enforcement, self- assessment reliance, and the need for local adaptation of global standards, recommending scalable, context-sensitive compliance models (Finch & Butt, 2025). Such frameworks serve as a blueprint influencing global regulatory trends.
Legal Challenges and Liability Frameworks for AI	AI's autonomous nature presents novel legal challenges, particularly for liability in sectors like healthcare, finance, and competition law. Indian laws, including the Information Technology Act, are inadequate for AI-specific issues, resulting in unclear accountability mechanisms. The EU and US are developing more robust liability regulations addressing these gaps. Research underscores the necessity for updated legal instruments to handle AI-induced harms, ensure sustainability, and promote responsible innovation. (Bose, 2025)

Global AI Governance and Multilateral Regulatory Trends	The global AI governance landscape is marked by diverse regional strategies ranging from the EU's comprehensive regulation to the US's decentralized model and China's state-led approach. International organizations and forums foster harmonization efforts emphasizing human rights, ethical AI, and innovation balance. The literature highlights the absence of binding international agreements, regulatory fragmentation, and the critical need for inclusive global frameworks to address AI's transnational challenges (Cornelius, 2025).
AI's Impact on Privacy and Data Protection	AI's integration raises acute concerns about data privacy, surveillance, and misuse, pressing legal systems to evolve data protection laws. The EU GDPR and AI Act contribute significantly to privacy safeguards, while India's recent Digital Personal Data Protection Act begins to fill gaps. Deepfake technology, biometric data risks, and automated decision-making necessitate privacy-centric regulatory responses to uphold individual rights (Raghuvanshi et al., 2025). The intersection of AI and privacy remains a dynamic and critical regulatory frontier.
AI in Justice and Constitutional Law	AI's deployment in judicial processes and constitutional rights spheres introduces efficiency gains alongside risks to transparency, fairness, and fundamental rights. The EU's legal frameworks emphasize accountability and human oversight in judicial AI applications, whereas India grapples with underdeveloped protections and judicial reinterpretation needs. Constitutional challenges include safeguarding equality, liberty, and dignity in AI's algorithmic decisions (Arora, 2025). This theme reflects a growing focus on aligning AI governance with rule of law principles.
Addressing Algorithmic Bias and Fairness in AI Systems	Algorithmic bias threatens fairness and equity, demanding legal and ethical remedies. Indian laws are criticized for lacking explicit AI bias mitigation measures, while the EU incorporates fairness into its regulatory and standards frameworks. Researchers advocate for bias auditing, transparency mandates, and integration of constitutional principles to ensure equitable AI deployment (Salaria et al., 2025). Efforts to mitigate bias reflect broader societal commitments to justice and non- discrimination.
Challenges of Regulatory Enforcement and Compliance for Diverse Actors	The complexity of AI governance creates asymmetries among stakeholders, particularly disadvantaging low-capacity actors like SMEs and public bodies. The EU AI Act's compliance requirements, while comprehensive, pose practical challenges in enforceability and proportionality. Literature suggests developing lightweight compliance frameworks and region-specific adaptations to democratize trustworthy AI governance (Finch & Butt, 2025). Addressing these challenges is crucial for equitable and effective regulatory outcomes.
AI's Influence on Market Regulation and Competition Law	AI-driven market behaviors, including algorithmic collusion and dominant platform practices, raise novel competition law concerns. India's Competition Act is scrutinized for its capacity to address such AI-specific challenges, with calls for AI-tailored competition guidelines. Comparative insights from the EU, US, and China inform policy proposals emphasizing transparency and data-sharing frameworks to preserve market fairness (S. Gupta, 2025). This emerging theme links AI regulation with economic sustainability and innovation balance.

2.4 Theoretical and Practical Implications

Theoretical Implications

- The synthesis of findings underscores the evolving nature of AI as a disruptive force challenging traditional legal and ethical paradigms, supporting theories that emphasize the need for adaptive, risk-based regulatory frameworks that integrate both technological and societal dimensions (Cornelius, 2025). This aligns with the EU's pioneering risk-tiered approach, which balances innovation with fundamental rights protection.
- The comparative analysis between the EU and India reveals theoretical divergence in regulatory maturity, with the EU exemplifying a comprehensive, rights-based model, while India's fragmented and sector-specific approach highlights gaps in operationalizing ethical AI governance (Kaur, 2025). This supports theoretical frameworks advocating for harmonized, human rights-centric AI regulation.
- Findings challenge existing legal theories that rely heavily on traditional liability and data protection laws, demonstrating their insufficiency in addressing AI-specific issues such as algorithmic bias, opacity, and autonomous decision-making (Singh, 2025). This calls for theoretical expansion to incorporate AI's unique characteristics into legal doctrines.
- The literature advances the theoretical discourse on the integration of ethics and law by emphasizing the necessity of embedding

human rights principles as a foundational element of AI governance, moving beyond voluntary ethical guidelines toward enforceable legal standards (Olariu & Zeleznikow, 2025).

- The global overview highlights the tension between policy-driven and market-driven regulatory models, suggesting a theoretical synthesis that combines hard law with soft law mechanisms to achieve both legitimacy and flexibility in AI legislation (Tang, 2025).
- The emerging scholarship on AI's impact on constitutional rights, particularly personality and privacy rights, extends theoretical understanding of how AI challenges classical legal concepts and necessitates reinterpretation within diverse constitutional frameworks (Arora, 2025).

Practical Implications

- For policymakers, the findings advocate for the adoption of comprehensive, risk- based AI regulatory frameworks akin to the EU AI Act, which effectively address ethical concerns such as transparency, accountability, and fundamental rights protection, while fostering innovation (Manchev, 2024). India's regulatory evolution would benefit from such a model to close legislative gaps and enhance enforcement.
- Industry stakeholders must prepare for increasing regulatory scrutiny, particularly in high-risk AI applications, by implementing robust compliance mechanisms including algorithmic transparency, bias auditing, and data protection measures to align with emerging global standards (Bose, 2025).
- The comparative insights emphasize the importance of international cooperation and harmonization of AI regulations to reduce fragmentation, facilitate market access, and ensure consistent ethical standards across jurisdictions (Matai, 2024). This is critical for multinational corporations and regulators alike.
- The practical challenges faced by low-capacity actors such as SMEs and public authorities in complying with complex AI regulations highlight the need for scalable, accessible compliance frameworks and capacity-building initiatives (Finch & Butt, 2025). This ensures equitable participation in AI governance and prevents regulatory exclusion.
- The integration of AI in sensitive sectors like healthcare, finance, and justice necessitates tailored legal frameworks that address sector-specific risks, liability issues, and ethical concerns, underscoring the need for interdisciplinary collaboration between AI practitioners, legal experts, and domain specialists (Sun et al., 2024).
- Finally, the findings stress the urgency for India to enact dedicated AI legislation that balances innovation with ethical governance, protects digital rights, and aligns with international best practices to foster trust and sustainable AI development in its rapidly growing digital economy (Kaur, 2025).

2.5 Limitations of the Literature

Area of Limitation	Description of Limitation
Geographic Bias	Many studies exhibit a Western-centric focus, limiting the external validity of findings across diverse cultural and regulatory contexts. This geographic bias restricts understanding of AI governance in underrepresented regions, affecting the generalizability of conclusions.
Lack of Consensus on Definitions	The absence of universally accepted definitions for key concepts such as "Artificial Intelligence," "transparency," and "fairness" introduces methodological constraints. This ambiguity complicates comparative analyses and weakens the coherence of regulatory and ethical frameworks.
Limited Empirical Data	The literature largely relies on qualitative, doctrinal, or normative analyses with scarce empirical or quantitative data. This methodological constraint reduces the robustness of findings and limits the assessment of real-world regulatory impacts and enforcement efficacy.
Fragmented Legal Frameworks	Several papers highlight the fragmented and evolving nature of AI regulation, especially in India, which lacks comprehensive AI-specific legislation. This fragmentation limits the ability to draw conclusive insights on regulatory effectiveness and complicates comparative analyses.
Limited Focus on Long-term Societal Impacts	Few studies adequately address the long-term societal consequences of AI deployment, such as job displacement and structural inequalities, which limit foresight in policy-making and ethical governance.
Rapidly Evolving Technology	The fast pace of AI technological advancements outstrips the slower development of legal frameworks, causing many studies to become quickly outdated. This temporal limitation affects the validity of conclusions regarding regulatory adequacy and future-proofing.

Limited Focus on Emerging AI Technologies	Emerging AI domains such as generative AI, deepfakes, and quantum AI receive limited coverage, restricting the literature's comprehensiveness and its ability to anticipate novel regulatory challenges posed by these technologies.
Insufficient Multidisciplinary Perspectives	The literature often lacks interdisciplinary collaboration, particularly integrating social sciences with technical AI research. This constraint limits understanding of AI's societal impacts and the development of nuanced, context-sensitive regulatory approaches.

2.6 Gaps and Future Research Directions

Gap Area	Description	Future Research Directions	Justification
Empirical Evaluation of Bias Mitigation Effectiveness	There is a lack of longitudinal and real-world empirical studies assessing the effectiveness of bias mitigation techniques across diverse sectors and contexts.	Conduct longitudinal, cross-sector empirical studies to evaluate the practical impact of bias mitigation strategies in AI systems, including healthcare, finance, and public administration, to develop standardized metrics for real-world bias reduction effectiveness.	Without empirical validation, bias mitigation techniques remain theoretical, limiting their adoption and trustworthiness in critical applications (Oguntibeju, 2024).
Multi-Stakeholder Transparency Needs and Communication	Current transparency mechanisms often fail to address the diverse needs of stakeholders, including technical experts, legal authorities, and affected public users.	Investigate communication strategies that enhance meaningful understanding without compromising proprietary information, and develop adaptive transparency frameworks that tailor explanations and disclosures to different stakeholder groups.	Transparency is not one-size-fits-all; mismatches between technical explanations and user comprehension undermine accountability and trust (Nuenen et al., 2020).
Global Regulatory Fragmentation and Harmonization Challenges	AI regulations vary widely across jurisdictions, with no binding international framework, causing legal uncertainty and competitive imbalances.	Explore pathways for international cooperation and harmonization of AI standards, including mutual recognition agreements and global ethical norms, focusing on India-EU alignment.	Fragmentation impedes cross-border AI governance and consistent rights protection (Gaho, 2024).
Operationalizing Ethical Principles into AI Law	Ethical principles like transparency, fairness, and accountability are often stated but poorly operationalized, especially in India, leading to risks of "ethics washing" and gaps between theory and practice.	Design and test practical frameworks and toolkits that translate ethical principles into actionable governance processes, including ethical audits, impact assessments, and compliance monitoring.	Without operationalization, ethical principles remain aspirational, undermining trust and allowing unethical AI deployment (Sun et al., 2024).
Accountability Attribution in Complex AI Ecosystems	Diffused responsibility among multiple actors in AI development and deployment creates ambiguity in accountability, especially in socio-technical systems.	Investigate frameworks for joint and layered accountability to develop computational and legal models for clear responsibility attribution in AI ecosystems, including roles for developers, operators, and third parties.	Ambiguity in accountability undermines legal recourse and ethical governance, particularly in complex AI systems (P.R. & Gayathri, 2024).
Integration of Human Rights Frameworks in AI Governance	Despite recognition of human rights relevance, their integration into AI governance remains limited and inconsistent.	Advance interdisciplinary research to embed human rights norms systematically into AI regulatory and ethical frameworks and develop assessment tools to evaluate AI compliance with human rights standards.	Human rights provide a robust, enforceable foundation for AI governance, addressing limitations of voluntary ethics (Arora, 2025).

Transparency-Explainability Trade-offs in Black-Box Models	Challenges persist in balancing model performance with transparency and explainability, especially in complex AI systems.	Investigate novel explainability techniques that preserve model accuracy while enhancing interpretability. Explore user-centric explainability approaches and their impact on trust and accountability.	Addressing the "transparency fallacy" is critical to ensure explanations are meaningful and actionable (Nannini, 2024).
Sector-Specific Governance Frameworks	Generic AI governance frameworks often overlook sector-specific risks and ethical challenges, limiting their effectiveness.	Develop tailored governance models for high-risk sectors such as finance, healthcare, and law enforcement, incorporating domain-specific ethical, legal, and technical considerations.	Sector-specific approaches improve relevance and compliance, addressing unique challenges and stakeholder needs (Chopra, 2024).
Addressing AI's Societal Impacts Beyond Legal Frameworks	Current AI regulations often react to issues post-facto and lack comprehensive approaches to societal impacts like job displacement and social equity.	Develop proactive, interdisciplinary regulatory strategies incorporating social science insights to anticipate and mitigate AI's broader societal effects.	Proactive regulation can reduce negative social consequences and enhance AI's societal benefits (Sun et al., 2024)
Enhancing Public Engagement and Awareness in AI Governance	Public understanding and involvement in AI governance remain limited, reducing legitimacy and accountability.	Design and evaluate participatory governance mechanisms, public education programs, and transparency initiatives that empower citizens to engage with AI decision-making processes.	Public trust and legitimacy depend on meaningful engagement and awareness of AI impacts and governance (Saxena, 2024).
Protection of Personality and Identity Rights in AI Contexts	AI-generated synthetic media challenge traditional personality rights, with India's legal protections being underdeveloped compared to the EU.	Conduct comparative legal research to formulate harmonized personality rights protections in India, addressing AI- specific challenges like deepfakes and digital identity misuse.	Robust personality rights are critical to prevent identity abuses and uphold dignity in the AI era (Arora, 2025).

2.7 Overall Synthesis and Conclusion

The collective body of literature reveals that emerging AI systems significantly challenge traditional legal and ethical frameworks by introducing complexities around privacy, accountability, bias, and fundamental rights protection. Globally, regulatory responses remain fragmented and uneven, with the European Union standing out for its comprehensive, risk-based AI regulatory framework that integrates robust ethical principles into enforceable legal mandates. The EU's AI Act exemplifies an advanced model that balances innovation with strong safeguards for transparency, human oversight, and rights protection, setting a global standard for AI governance. Its tiered risk approach, extensive enforcement mechanisms, and alignment with data protection laws like the GDPR contribute to a cohesive system that operationalizes ethical AI in practice.

In contrast, India's AI regulatory landscape is characterized by fragmentation, sector- specific policies, and the absence of a dedicated AI law, resulting in legislative gaps, unclear accountability, and weaker enforcement capabilities. While recent steps such as the Digital Personal Data Protection Act signal progress toward enhanced privacy safeguards, India's framework generally lacks the cohesion and specificity necessary to fully address AI's multifaceted ethical and legal challenges. The Indian legal system struggles with translating constitutional principles into actionable AI governance, particularly concerning algorithmic bias, data privacy, and liability in critical sectors like healthcare and finance. This regulatory uncertainty poses risks to innovation and fundamental rights alike, underscoring the need for comprehensive, context-sensitive legislation that is informed by global best practices but tailored to India's socio-legal realities.

Globally, the literature highlights the necessity of harmonizing diverse regulatory architectures through international cooperation and adaptive frameworks that accommodate local values while upholding universal ethical standards. Enforcement remains a pervasive challenge worldwide, especially for smaller actors and jurisdictions relying on self-regulation or soft law. Inclusive governance approaches that consider capacity disparities alongside technological innovation are essential to ensure equitable compliance and rights protection. Overall, the synthesis underscores the imperative for jurisdictions like India to develop integrated, enforceable AI regulatory frameworks inspired by the EU's risk-based model but adapted to domestic contexts, to effectively safeguard fundamental rights, promote accountability, and foster responsible innovation in the rapidly evolving AI landscape.

3. METHODOLOGY

3.1 Research Design

This study employed a qualitative, interdisciplinary research design, drawing on comparative analysis across law, ethics, and computer science. The design is intentionally exploratory, aiming to highlight both convergence and tension among different frameworks, and to identify practical implications for governance – it was structured as an interdisciplinary synthesis of legal analysis, ethical framework evaluation, and technical assessment to address the complex intersection of algorithmic accountability, transparency, and fairness in AI systems. This approach is particularly suited to emerging fields like AI regulation, where empirical data remain limited but conceptual clarity and cross-disciplinary dialogue are essential.

3.2 Scope of Study

The scope of this research is focused on the comparative analysis of AI regulatory frameworks in India and the EU, highlighting their approaches to risk management, legal enforceability, and ethical standards. The paper integrates principles of transparency, accountability, and human rights protection to draw contrast and emphasize the need for regulatory mechanisms that ensure ethical AI deployment while fostering innovation

3.3 Data Sources

The research draws primarily on secondary data. A comprehensive literature search was conducted across multiple academic databases to ensure interdisciplinary coverage – Westlaw and LexisNexis for papers focused on legal aspects; OECD iLibrary and government repositories for governance and policy insights; PhilPapers and Project MUSE for philosophical and ethical discussions; and Research Gate, Mendeley, JSTOR, and Science Direct for multidisciplinary and social science-oriented papers

Academic journal articles, research examining legal frameworks for AI regulation, technical papers on explainable AI with governance implications, reports by international organizations, and studies addressing AI accountability, transparency, or ethical governance, supplemented by multi-jurisdictional or comparative studies, form the core material. This combination ensures both scholarly depth and practical relevance.

3.4 Limitations

Several limitations shape the findings of this study. First, the reliance on secondary sources means the analysis depends on the quality and completeness of existing literature, which is itself uneven across regions and disciplines, and quickly limited in relevance due to the rapid evolution of AI and its governance. Second, geographic representation is skewed toward Western contexts, reflecting broader patterns in AI scholarship and governance, while differences in legal systems limit the generalizability of comparative findings. Third, the absence of original empirical data restricts the ability to evaluate how proposed frameworks function in real-world settings. Finally, definitional ambiguities—particularly around terms such as “fairness” and “transparency”—introduce interpretive challenges that complicate cross-comparison.

3.5 Strengths

Despite these limitations, the study offers several strengths. Its interdisciplinary lens allows for a richer understanding of algorithmic accountability than could be achieved from a single field alone. The comparative approach highlights both shared challenges and jurisdiction-specific nuances, offering insights that are transferable across contexts. By synthesizing legal, ethical, and technical perspectives, the study provides a well-rounded foundation for policymakers, practitioners, and researchers seeking to design governance frameworks that are both principled and practical. Moreover, its attention to global perspectives helps counterbalance the dominance of Western-centric narratives in AI governance debates.

4. AI SURVEILLANCE AND THE RIGHT TO PRIVACY

4.1 Conceptual Framework and Legal Foundations

AI-enabled surveillance systems represent one of the most contested applications of artificial intelligence, raising fundamental questions about the balance between security, efficiency, and individual privacy rights. The deployment of automated monitoring technologies—including CCTV networks with facial recognition, predictive policing algorithms, and behavioural analytics platforms—has prompted distinct regulatory responses in the EU and India (Y. Gupta, 2025).

The EU's approach to AI surveillance is anchored in the GDPR's comprehensive data protection framework, which treats surveillance activities as high-risk processing requiring enhanced safeguards. The GDPR establishes that any processing of personal data, including through AI systems, must satisfy one of six lawful bases (consent, contract, legal obligation, vital interests, public task, or legitimate interests) as specified in Article 6 (Kishwar et al., 2025). For surveillance applications that involve systematic monitoring or automated decision-making with significant effects, Articles 35 and 36 mandate Data Protection Impact Assessments (DPIAs) and, where necessary, prior consultation with supervisory authorities (Sriram et al., 2024).

India's regulatory trajectory has been more complex and evolutionary. Prior to the DPDP Act 2023, India relied on a patchwork of sectoral regulations, constitutional privacy jurisprudence (notably the *K.S. Puttaswamy v. Union of India* judgment recognizing

privacy as a fundamental right), and the Information Technology Act 2000 (Yadav & Sharma, 2025). The DPDP Act represents India's first comprehensive data protection statute, incorporating elements inspired by the GDPR while reflecting distinct national priorities. However, the Act contains broader exemptions for state processing in the interests of sovereignty, security, and public order, creating a more permissive environment for government surveillance activities compared to the EU framework (Jain, 2022).

4.2 Regulatory Requirements and Safeguards

EU GDPR Framework:

The GDPR imposes multiple layers of protection for AI surveillance systems:

1. **Privacy by Design and Default (Article 25):** Controllers must implement technical and organizational measures to ensure that processing meets GDPR requirements and protects data subject rights from the outset. For surveillance systems, this translates to requirements for data minimization, purpose limitation, and built-in privacy safeguards.
2. **Data Protection Impact Assessments (Article 35):** DPIAs are mandatory for processing operations likely to result in high risk to individuals' rights, explicitly including systematic monitoring of publicly accessible areas on a large scale and automated decision-making with legal or similarly significant effects. The DPIA process requires controllers to describe the processing, assess necessity and proportionality, identify risks, and propose mitigation measures.
3. **Lawfulness and Transparency:** Surveillance activities must satisfy stringent lawfulness requirements, with particularly high standards for public authority processing. The GDPR's transparency obligations (Articles 12-14) require clear information about surveillance activities, though exceptions exist for law enforcement purposes under specific conditions (Kishwar et al., 2025).
4. **Data Subject Rights:** Individuals retain rights to access, rectification, erasure, and objection even in surveillance contexts, subject to limited exceptions for law enforcement and national security.

India's DPDP Framework:

The DPDP Act 2023 introduces several provisions relevant to surveillance, though with notable differences from the GDPR:

1. **Purpose Limitation and Transparency:** The Act requires data fiduciaries to process personal data lawfully, for specified purposes, and with appropriate transparency. However, the specificity of these obligations and their application to surveillance contexts await clarification through subordinate rules.
2. **State Exemptions:** Sections 17 and 18 of the DPDP Act provide broad exemptions for government processing in the interests of sovereignty, security, public order, and friendly relations with foreign states. These exemptions significantly limit the Act's constraints on state surveillance activities, creating a fundamental divergence from the GDPR's more circumscribed public interest exceptions.
3. **Risk Assessment Obligations:** While the DPDP Act contemplates safeguards for high-risk processing, the detailed requirements for impact assessments analogous to GDPR DPIAs are left to future regulations. This creates uncertainty about the practical constraints on deploying AI surveillance systems.
4. **Data Principal Rights:** The Act provides rights similar to GDPR data subject rights, including rights to access, correction, and erasure. However, these rights are subject to the broad state exemptions mentioned above.

4.3 Comparative Analysis: Key Differences and Similarities

Dimension	EU GDPR	India DPDP Act 2023
Legal Basis	Six specific lawful bases; legitimate interests require balancing test; explicit consent for sensitive data	Lawful processing required but bases less precisely defined; awaiting subordinate rules
Risk Assessment	Mandatory DPIAs for high-risk processing including systematic monitoring; detailed procedural requirements	Risk assessment framework contemplated but details deferred to regulations
State Surveillance	Limited public interest exceptions; law enforcement processing subject to LED (Law Enforcement Directive); strong judicial oversight	Broad exemptions for sovereignty, security, and public order; weaker constraints on state surveillance
Transparency	Detailed transparency obligations with limited exceptions	Transparency required but scope and exceptions unclear pending rules
Independent Oversight	Strong, independent supervisory authorities with investigative and enforcement powers	Data Protection Board established but powers and independence to be tested in practice
Cross-border Implications	Adequacy decisions govern transfers; SCCs and BCRs available	EU adequacy unlikely under current framework; transfers may require additional safeguards

Convergence: Both frameworks recognize privacy as a fundamental right and establish principles of lawfulness, purpose limitation, and data minimization. Both contemplate enhanced protections for high-risk AI processing and provide individual rights of access and correction.

Divergence: The most significant divergence lies in the treatment of state surveillance. The GDPR, supplemented by the Law Enforcement Directive and CJEU jurisprudence (e.g., *Schrems II*), imposes meaningful constraints on government surveillance and requires robust judicial oversight. India's DPDP Act, by contrast, contains broad state exemptions that substantially limit its application to government surveillance activities. Additionally, the EU's established supervisory architecture and enforcement mechanisms contrast with India's nascent regulatory infrastructure, raising questions about practical implementation and compliance.

4.4 Scholarly Perspectives and Implementation Challenges

Scholars have identified several critical challenges in applying data protection frameworks to AI surveillance:

Opacity and Complexity: AI surveillance systems, particularly those employing deep learning, often function as "black boxes" that resist meaningful explanation. This opacity undermines the effectiveness of transparency obligations and individual rights (Sriram et al., 2024). DPIAs and privacy-by-design requirements are valuable but imperfect tools for addressing these challenges, as they depend on the availability of technical expertise and the willingness of controllers to prioritize privacy over functionality (Sriram et al., 2024).

Collective Harms: Traditional data protection frameworks, including both the GDPR and DPDP Act, are structured around individual rights and harms. However, AI surveillance systems generate collective risks—discriminatory patterns, chilling effects on public behaviour, and erosion of democratic norms—that individual remedies cannot adequately address (Sriram et al., 2024). Scholars argue for governance mechanisms beyond individual consent and access rights, including algorithmic auditing, public participation in deployment decisions, and sector-specific regulations (Y. Gupta, 2025).

Enforcement Gaps: Even in the EU, enforcement of GDPR obligations for AI surveillance has been inconsistent. Supervisory authorities face resource constraints, technical complexity, and political pressure when investigating government deployments. In India, the effectiveness of the Data Protection Board remains to be demonstrated, and the interaction between the DPDP Act, sectoral regulations, and Aadhaar-era surveillance systems creates regulatory complexity (Yadav & Sharma, 2025).

Balancing Security and Privacy: Both jurisdictions grapple with the challenge of balancing legitimate security interests against privacy rights. The EU's approach, emphasizing necessity, proportionality, and judicial oversight, contrasts with India's broader state exemptions. This difference reflects divergent political contexts and priorities but raises concerns about the potential for surveillance overreach in the Indian context (Yadav & Sharma, 2025).

4.5 Case Studies and Practical Implementations

EU Context:

- **Public Space Surveillance:** Several EU member states have deployed or piloted facial recognition systems in public spaces, triggering DPIA requirements and supervisory scrutiny. For example, the use of facial recognition by law enforcement agencies has been subject to strict conditions and, in some cases, moratoria or bans (e.g., temporary bans in certain cities) pending clearer legal frameworks (Kishwar et al., 2025).
- **Supervisory Enforcement:** EU data protection authorities have issued guidance on AI and surveillance, conducted investigations into unlawful deployments, and imposed penalties for GDPR violations. However, the fragmentation of enforcement across member states and the limited public disclosure of DPIAs limit comprehensive assessment (Sriram et al., 2024).

India Context:

- **Aadhaar and Biometric Surveillance:** India's Aadhaar system, the world's largest biometric identification program, exemplifies the tension between service delivery efficiency and privacy rights. The Supreme Court's *Aadhaar* judgment (2018) upheld the system's constitutional validity while imposing some limitations, but concerns about surveillance potential and data security persist (Sharma & Sharma, 2024).
- **Facial Recognition Deployments:** Indian law enforcement agencies and state governments have deployed facial recognition systems for purposes including criminal identification, crowd monitoring, and COVID-19 contact tracing. These deployments have occurred with limited public transparency, minimal regulatory oversight, and contested legality under pre-DPDP frameworks. The applicability of DPDP Act safeguards to these systems remains unclear given state exemptions (Y. Gupta, 2025).
- **Smart City Initiatives:** India's Smart Cities Mission includes extensive surveillance infrastructure, raising questions about data protection, consent, and purpose limitation. The interaction between municipal surveillance systems, the DPDP Act, and sectoral regulations awaits practical clarification (Sharma & Sharma, 2024).

Comparative Insights:

The case studies reveal that both jurisdictions face implementation challenges, but the nature of these challenges differs. In the EU, the primary issues are enforcement consistency, technical capacity for meaningful DPIAs, and political will to constrain government surveillance. In India, the challenges are more foundational: establishing effective regulatory institutions, operationalizing DPDP Act principles through subordinate rules, and addressing the tension between broad state exemptions and meaningful privacy protection.

5. CONSENT AND DATA OWNERSHIP IN MACHINE LEARNING SYSTEMS

5.1 The Consent Paradigm in AI/ML Contexts

Consent has long served as a cornerstone of data protection law, embodying the principle of individual autonomy and informational self-determination. However, the application of traditional consent frameworks to machine learning systems reveals fundamental tensions between legal requirements and technical realities.

Machine learning systems, particularly those employing deep neural networks, process vast datasets to identify patterns and generate predictions or classifications. The scale, complexity, and unpredictability of ML processing challenge the feasibility of obtaining meaningful, informed consent. Key difficulties include:

1. **Scope and Granularity:** ML training datasets may contain millions or billions of data points from diverse sources. Obtaining individual consent for each data point and each potential use is practically infeasible.
2. **Unpredictability of Downstream Uses:** ML models trained for one purpose may be repurposed, fine-tuned, or combined with other models for unforeseen applications. The open-ended nature of potential uses undermines the specificity required for valid consent.
3. **Informational Complexity:** Explaining the technical operation of ML algorithms, the inferences they may generate, and the risks they pose requires a level of detail that exceeds most individuals' technical literacy and attention capacity. This creates what scholars term the "transparency fallacy"—legalistic disclosures that satisfy formal requirements but fail to enable meaningful understanding.
4. **Withdrawal and Erasure:** Even where consent is initially obtained, exercising the right to withdraw consent or request erasure after data has been incorporated into a trained model raises complex technical and legal questions. While some techniques (e.g., machine unlearning) are being developed, they remain imperfect and computationally expensive.

5.2 EU GDPR Framework for Consent in ML

Legal Requirements:

The GDPR establishes rigorous standards for valid consent in Article 7, requiring that consent be:

- **Freely given:** Without coercion, deception, or significant imbalance of power
- **Specific:** Tied to particular, well-defined purposes
- **Informed:** Based on clear, accessible information about processing activities
- **Unambiguous:** Manifested through affirmative action, not silence or pre-ticked boxes

For ML systems processing special category data (Article 9), explicit consent is generally required unless another lawful basis applies (e.g., substantial public interest, scientific research with safeguards) (Kishwar et al., 2025).

Alternative Lawful Bases:

Recognizing the limitations of consent for ML applications, the GDPR provides alternative lawful bases that are often more appropriate:

- **Legitimate Interests (Article 6(1)(f)):** Controllers may rely on legitimate interests where processing is necessary for their interests or those of third parties, subject to a balancing test against data subjects' rights. This basis is frequently invoked for ML applications in commercial contexts.
- **Public Task and Legal Obligation:** Government and research institutions may process data for public interest or legal compliance purposes, subject to appropriate safeguards.
- **Scientific Research Exemptions:** Article 89 provides derogations for scientific research, including relaxed requirements for purpose limitation and consent withdrawal, provided appropriate safeguards (e.g., anonymization, pseudonymization) are implemented.
- **Rights-Based Governance:** Beyond consent, the GDPR employs a suite of data subject rights and controller obligations to govern ML processing:
- **Right to Explanation (Article 22):** Individuals have the right not to be subject to solely automated decisions with legal or similarly significant effects, and the right to obtain meaningful information about the logic involved. However, scholars debate whether this right provides effective recourse against complex ML systems.

- **Data Protection Impact Assessments:** As discussed in Section 1, DPIAs are required for high-risk ML processing and serve as a key governance mechanism beyond individual consent.
- **Data Minimization and Purpose Limitation:** Articles 5(1)(b) and 5(1)(c) require that data collection be adequate, relevant, and limited to what is necessary for specified purposes. These principles constrain the scope of ML training data.

Scholarly Critique:

Legal scholars and technologists have argued that the GDPR's consent framework is ill-suited to ML realities. Edwards and Veale (2017) contend that the "right to explanation" is unlikely to provide meaningful remedy given the technical opacity of ML systems and the limited utility of post-hoc explanations. Others emphasize that individual consent cannot address collective harms from ML systems and that governance must shift toward systemic oversight, algorithmic auditing, and purpose limitation rather than consent-based legitimation (Sriram et al., 2024).

5.3 India's Consent Framework and Data Ownership

DPDP Act 2023 Provisions:

The DPDP Act incorporates consent as a central principle but with notable differences from the GDPR:

1. **Consent Requirements:** Section 6 requires that consent be free, specific, informed, and unambiguous, mirroring GDPR language. However, the Act provides less detailed guidance on operationalizing these requirements, leaving critical details to subordinate rules.
2. **Notice and Transparency:** Data fiduciaries must provide clear notice of processing purposes, data retention periods, and rights available to data principals. The specificity and enforceability of these obligations await regulatory clarification (Yadav & Sharma, 2025).
3. **Exemptions and Alternatives:** The DPDP Act includes exemptions for legitimate uses (e.g., processing for specified public purposes, compliance with legal obligations) and broad state exemptions that significantly narrow the Act's scope.
4. **Children's Data:** The Act includes specific provisions for processing children's data, requiring verifiable parental consent. The practical implementation of age verification and parental consent mechanisms for ML applications remains uncertain.

Data Ownership and Control:

The concept of "data ownership" is legally and philosophically contested. Neither the GDPR nor the DPDP Act establishes a property-rights model of data ownership. Instead, both frameworks prioritize:

- **Control Rights:** Data subjects/principals have rights to access, correct, and erase their data, but not absolute ownership in the sense of property law.
- **Controller/Processor Obligations:** The frameworks impose obligations on entities that determine the purposes and means of processing (controllers) and those that process on behalf of controllers (processors), but do not vest ownership in individuals.
- **Derived Data and Models:** The legal status of ML models trained on personal data, and the inferences or predictions generated by such models, remains ambiguous. Are models "personal data" if they encode information about individuals? Do individuals have rights over inferences drawn about them? These questions lack clear answers in both jurisdictions.

Comparative Perspectives:

Determann and Gupta (2020) compare India's draft data protection legislation (predecessor to the DPDP Act) with the GDPR and California Consumer Privacy Act, noting that India's framework reflects a hybrid approach: incorporating EU-style data subject rights while maintaining flexibility for developmental priorities and state interests. The DPDP Act continues this hybrid approach, but the practical implications for ML consent and ownership await implementation experience.

5.4 Challenges in Obtaining Meaningful Consent for ML Training Data

Scale and Complexity:

Modern ML systems are trained on datasets that may include billions of data points from diverse sources—web scraping, user-generated content, sensor data, purchased datasets, and more. The provenance of training data is often opaque, making it difficult to trace whether consent was obtained for each data point and for the specific ML application.

Unpredictable Downstream Uses:

ML models trained for one purpose (e.g., image classification) may be repurposed for other applications (e.g., facial recognition, emotion detection) through transfer learning or fine-tuning. The open-ended potential for model reuse undermines the purpose specificity required for valid consent under both GDPR and DPDP frameworks.

Information Asymmetry and Complexity:

Explaining ML processing in terms accessible to laypeople is extraordinarily difficult. Disclosures must convey not only what data is collected but also how it will be processed, what inferences may be drawn, and what risks may arise—all in the context of probabilistic, non-deterministic systems. Research indicates that even detailed disclosures often fail to enable meaningful understanding, leading to "consent theatre" that satisfies formal requirements without empowering individuals (Sriram et al., 2024).

Technical Mitigation Strategies:

Researchers have proposed technical approaches to mitigate consent challenges:

- **Data Minimization and Anonymization:** Limiting data collection to what is necessary and anonymizing or pseudonymizing data can reduce privacy risks, though anonymization is increasingly difficult given re-identification techniques.
- **Differential Privacy:** Adding calibrated noise to datasets or model outputs can provide mathematical privacy guarantees, enabling ML training while limiting individual privacy risks. However, differential privacy involves utility trade-offs and requires careful parameter selection.
- **Federated Learning:** Training models on decentralized data without centralizing datasets can reduce privacy risks, though federated learning introduces its own challenges (e.g., model inversion attacks, communication overhead).
- **Machine Unlearning:** Techniques to remove the influence of specific data points from trained models are being developed to operationalize the right to erasure, but remain computationally expensive and imperfect.

Regulatory Responses:

Both the EU and India face the challenge of adapting consent frameworks to ML realities. Potential regulatory responses include:

- **Shifting from Consent to Purpose Limitation:** Emphasizing strict purpose limitation and use restrictions rather than granular consent for every processing activity.
- **Algorithmic Impact Assessments:** Requiring systematic risk assessments for ML systems, analogous to DPIAs, with public transparency and stakeholder input
- **Sector-Specific Regulations:** Developing tailored rules for high-risk ML applications (e.g., healthcare, finance, law enforcement) that reflect domain-specific risks and values.
- **Collective Governance Mechanisms:** Exploring data trusts, data cooperatives, and other collective governance models that move beyond individual consent to enable group decision-making about data use.

5.5 Data Ownership Models and Legal Implications

Conceptual Frameworks:

The notion of "data ownership" invokes property-law concepts but faces significant conceptual and practical challenges when applied to personal data and ML models:

1. **Property Rights Model:** Treating data as property that individuals own and can transfer, license, or sell. This model is attractive for its clarity but faces criticism for commodifying personal information and failing to account for the relational and contextual nature of privacy (Determann & Gupta, 2020).
2. **Rights-Based Model:** The approach adopted by GDPR and DPDP Act, which grants individuals specific rights (access, correction, erasure) without establishing full ownership. This model prioritizes control and autonomy without commodification.
3. **Stewardship Model:** Positioning data fiduciaries/controllers as stewards with obligations to process data responsibly, rather than as owners. This model emphasizes accountability and ethical obligations.

Legal Implications in EU and India:

- **Personal Data:** Both GDPR and DPDP Act treat personal data as subject to individual rights and controller obligations, not as property owned by either party. Individuals have control rights but cannot "sell" their data in the sense of transferring ownership.
- **ML Models:** The legal status of trained ML models is ambiguous. Models may embody trade secrets and intellectual property of the controller, but if they encode personal information or enable re-identification, they may also be subject to data protection obligations. Neither jurisdiction has definitively resolved whether and when models constitute "personal data" (Sriram et al., 2024).
- **Inferences and Derived Data:** Predictions, classifications, and inferences generated by ML systems raise novel questions. Are inferences "personal data" subject to data subject rights? Do individuals have ownership claims over inferences about them? GDPR Recital 26 suggests that anonymous information is outside the regulation's scope, but the line between personal and anonymous data is increasingly blurred.

Cross-Border Implications:

The divergence between EU and Indian approaches to data ownership and control has significant implications for cross-border data flows and ML system development:

- **Adequacy Decisions:** The European Commission assesses whether third countries provide "adequate" data protection to enable unrestricted data transfers. India's DPDP Act, with its broad state exemptions and nascent enforcement infrastructure, is unlikely to receive an adequacy decision in its current form.
- **Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs):** In the absence of adequacy, transfers from the EU to India must rely on SCCs, BCRs, or other safeguards. The *Schrems II* decision underscores that such mechanisms require case-by-case assessment of the destination country's surveillance laws, raising challenges for EU-India data flows ((Jain, 2022).
- **Practical Compliance:** Multinational organizations developing ML systems must navigate divergent consent requirements, data localization provisions (not addressed in detail here), and enforcement risks across jurisdictions.

6. BIOMETRIC DATA REGULATION AND FACIAL RECOGNITION TECHNOLOGIES

6.1 The Special Status of Biometric Data

Biometric data—including fingerprints, facial images, iris scans, voiceprints, and gait patterns—occupies a unique position in data protection law due to its sensitivity, permanence, and identification potential. Unlike passwords or PINs, biometric identifiers cannot be easily changed if compromised, and their collection often occurs without explicit awareness or consent (e.g., facial images captured by surveillance cameras) (Sharma & Sharma, 2024).

The use of biometric data in AI systems, particularly facial recognition technologies (FRT), has emerged as one of the most controversial applications of machine learning. FRT systems analyse facial features to verify identity (one-to-one matching) or identify individuals from databases (one-to-many matching), with applications ranging from smartphone unlocking to mass surveillance. The deployment of FRT raises acute concerns about privacy, discrimination, function creep, and the chilling effect on public behaviour (Y. Gupta, 2025).

6.2 EU Regulatory Framework for Biometric Data

GDPR Special Category Protection:

The GDPR classifies biometric data used for unique identification as "special category data" under Article 9, subjecting it to heightened protection. Processing of special category data is prohibited unless one of the specific conditions in Article 9(2) applies, including:

- **Explicit consent:** The data subject has given explicit consent for specified purposes
- **Substantial public interest:** Processing is necessary for substantial public interest reasons, subject to appropriate safeguards and legal basis in EU or member state law
- **Vital interests:** Processing is necessary to protect vital interests where the data subject is incapable of giving consent
- **Legitimate activities:** Processing by foundations, associations, or non-profit bodies for legitimate activities with appropriate safeguards

The heightened standard of "explicit consent" for biometric data contrasts with the general consent requirement for ordinary personal data, reflecting the sensitivity of biometric identifiers (Kishwar et al., 2025).

Data Protection Impact Assessments:

As discussed in Section 1, DPIAs are mandatory for processing operations likely to result in high risk, explicitly including biometric data processing for unique identification and systematic monitoring of publicly accessible areas. For FRT systems, this means controllers must:

- Describe the system's purpose, functionality, and data flows
- Assess the necessity and proportionality of processing
- Identify risks to data subjects (misidentification, discrimination, surveillance, function creep)
- Propose technical and organizational measures to mitigate risks
- Consult with supervisory authorities where residual risks remain high

Additional Safeguards:

- **Privacy by Design:** FRT systems must incorporate privacy safeguards from the outset, including data minimization, pseudonymization where possible, and access controls.
- **Transparency:** Data subjects must be informed about FRT processing, though exceptions exist for law enforcement and national security purposes.
- **Automated Decision-Making Safeguards:** Article 22 provides that individuals have the right not to be subject to solely automated decisions with legal or similarly significant effects, including the right to human intervention and the right to contest decisions. However, the practical application of this right to FRT systems is contested (Edwards & Veale, 2017).

Law Enforcement Directive (LED):

For FRT use by law enforcement and criminal justice authorities, the LED (Directive 2016/680) provides a parallel framework with specific safeguards, including requirements for legal basis, necessity, proportionality, and independent supervisory oversight.

Proposed AI Act:

The European Commission's proposed Artificial Intelligence Act (under negotiation as of 2023-2025) would further regulate FRT by:

- Prohibiting real-time remote biometric identification in publicly accessible spaces by law enforcement, subject to narrow exceptions for serious crimes
- Classifying post-real-time (retrospective) FRT as high-risk, triggering conformity assessment, risk management, and transparency requirements
- Requiring fundamental rights impact assessments for high-risk AI systems

6.3 India's Approach to Biometric Data Protection

Aadhaar: A Unique Context:

India's regulatory approach to biometric data is profoundly shaped by the Aadhaar system, launched in 2009 to provide a unique 12-digit identification number to all residents based on biometric (fingerprint and iris) and demographic data. Aadhaar has enrolled over 1.3 billion individuals, making it the world's largest biometric database (Sharma & Sharma, 2024).

The Supreme Court's landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2018) upheld Aadhaar's constitutional validity while imposing limitations:

- Aadhaar could be used for government subsidies, benefits, and services funded by the Consolidated Fund of India
- Private entities could not mandate Aadhaar for service provision (with limited exceptions)
- Safeguards against data misuse and unauthorized access were required
- The right to privacy, recognized as a fundamental right under Articles 14, 19, and 21 of the Constitution, constrained Aadhaar's scope.

However, subsequent amendments and regulations have expanded Aadhaar's permissible uses, and concerns about data security, unauthorized access, and function creep persist.

DPDP Act 2023 Provisions:

The DPDP Act does not explicitly classify biometric data as a special category requiring heightened protection, in contrast to the GDPR. However, several provisions are relevant:

1. **Sensitive Personal Data:** While the Act does not use the term "sensitive personal data," it contemplates enhanced protections for certain categories of data through subordinate rules. Whether and how biometric data will be treated as sensitive awaits regulatory clarification.
2. **Purpose Limitation and Data Minimization:** The Act's general principles of purpose limitation and data minimization apply to biometric data, but their practical enforcement in the context of large-scale biometric systems like Aadhaar remains uncertain.
3. **State Exemptions:** Sections 17 and 18 provide broad exemptions for government processing for sovereignty, security, and public order purposes. These exemptions significantly limit the DPDP Act's constraints on state biometric surveillance.
4. **Data Principal Rights:** Individuals have rights to access, correct, and erase their data, but the application of these rights to biometric identifiers (which are often permanent and used for authentication) raises practical challenges.

Sectoral Regulations:

In addition to the DPDP Act, biometric data in India is subject to sectoral regulations:

- **Aadhaar Act 2016:** Governs the collection, storage, and use of biometric data for Aadhaar purposes, with specific security and access control requirements.
- **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011:** Classify biometric information as sensitive personal data, requiring enhanced security measures and consent for collection.

The interaction between the DPDP Act, the Aadhaar Act, and sectoral rules creates a complex regulatory landscape with uncertain boundaries and potential conflicts.

6.4 Facial Recognition Technology: Comparative Regulation

EU Approach:

The EU's approach to FRT is characterized by caution and emphasis on fundamental rights:

- **High-Risk Classification:** FRT for identification purposes is treated as high-risk processing under the GDPR, triggering DPIAs, transparency obligations, and supervisory scrutiny.
- **Moratoria and Bans:** Several EU member states and cities have imposed temporary moratoria or bans on FRT use by law enforcement and public authorities, pending clearer legal frameworks and impact assessments. The European Parliament has called for a ban on biometric mass surveillance (Y. Gupta, 2025).
- **Judicial Oversight:** Courts and supervisory authorities have scrutinized FRT deployments for compliance with necessity, proportionality, and data protection principles. The CJEU's jurisprudence on data retention and surveillance (e.g., *Digital Rights Ireland*, *Tele2*) establishes high standards for justifying intrusive processing.
- **Proposed AI Act Restrictions:** As noted above, the proposed AI Act would prohibit real-time remote biometric identification by law enforcement in public spaces, with narrow exceptions, and classify post-real-time FRT as high-risk (Kishwar et al., 2025).

India Approach:

India's approach to FRT is characterized by more permissive deployment and less developed regulatory constraints:

- **Widespread Deployment:** Indian law enforcement agencies, state governments, and private entities have deployed FRT systems for purposes including criminal identification, crowd monitoring, airport security, and attendance tracking. Notable examples include the National Automated Facial Recognition System (AFRS) for law enforcement and FRT use during protests and public events (Y. Gupta, 2025).

- **Limited Transparency and Oversight:** Many FRT deployments have occurred with minimal public transparency, limited regulatory oversight, and uncertain legal basis. Civil society organizations have raised concerns about the lack of impact assessments, consent mechanisms, and safeguards against misuse (Sharma & Sharma, 2024).
- **DPDP Act Applicability:** The DPDP Act's applicability to government FRT systems is constrained by the broad state exemptions in Sections 17 and 18. Whether and how the Act's principles (purpose limitation, data minimization, transparency) will be enforced for FRT awaits practical experience and subordinate regulations.
- **Aadhaar and FRT Integration:** There are ongoing debates about the potential integration of FRT with Aadhaar's biometric database, which would create an unprecedented identification and surveillance capability. The legal and constitutional constraints on such integration remain contested.

Comparative Insights:

Dimension	EU	India
Legal Classification	Biometric data as special category; explicit consent or specific lawful basis required	No explicit special category status in DPDP Act; sectoral rules classify as sensitive
FRT Regulation	High-risk processing; DPIAs mandatory; proposed AI Act restrictions on real-time use	Limited regulatory constraints; broad state exemptions; widespread deployment
Transparency	Strong transparency obligations; public debate and civil society scrutiny	Limited transparency for government deployments; growing civil society advocacy
Independent Oversight	Established supervisory authorities; judicial review	Data Protection Board newly established; oversight effectiveness to be demonstrated
Enforcement	Significant enforcement powers and penalties; growing body of case law	Enforcement mechanisms under DPDP Act untested; sectoral enforcement fragmented

6.5 Enforcement Mechanisms and Penalties

EU Enforcement:

The GDPR establishes a robust enforcement architecture:

- **Supervisory Authorities:** Each member state has an independent supervisory authority with investigative, corrective, and sanctioning powers. Authorities can conduct audits, issue warnings and reprimands, order processing bans, and impose administrative fines.
- **Administrative Fines:** Violations can result in fines up to €20 million or 4% of annual global turnover, whichever is higher. Special category data violations (Article 9) and failure to conduct DPIAs (Article 35) are subject to the higher fine tier (Kishwar et al., 2025).
- **Private Enforcement:** Data subjects can bring complaints to supervisory authorities and pursue judicial remedies, including compensation for material and non-material damages (Article 82).
- **Enforcement Record:** EU supervisory authorities have issued significant fines and corrective orders for data protection violations, including cases involving biometric data and surveillance systems. However, enforcement has been uneven across member states, and resource constraints limit the scope of supervisory activities (Sriram et al., 2024).

India Enforcement:

The DPDP Act 2023 establishes a new enforcement framework:

- **Data Protection Board:** The Act creates a Data Protection Board of India with powers to investigate complaints, conduct inquiries, and impose penalties. The Board's composition, independence, and operational effectiveness remain to be demonstrated in practice.
- **Penalties:** The Act provides for penalties up to ₹250 crore (approximately €27 million or $30 million) for serious violations, including failure to implement reasonable security safeguards and processing in breach of Act provisions. However, the penalty framework is less detailed than the GDPR's tiered approach.
- **Private Enforcement:** Data principals can file complaints with the Data Protection Board, but the Act does not provide an explicit right to compensation analogous to GDPR Article 82. The availability and effectiveness of judicial remedies await clarification.
- **Enforcement Challenges:** India's enforcement infrastructure faces several challenges: the Data Protection Board is newly established and its capacity, independence, and resources are uncertain; the interaction between the Board, sectoral regulators, and judicial authorities is unclear; and the broad state exemptions limit the Board's jurisdiction over government processing.

Comparative Enforcement Analysis:

The EU's enforcement architecture is more mature, with established supervisory authorities, a growing body of case law, and demonstrated willingness to impose significant penalties. The GDPR's two-tiered fine structure and explicit compensation rights provide strong deterrents and remedies.

India's enforcement framework is nascent and faces structural challenges. The Data Protection Board's effectiveness will depend on its independence, resources, and political support. The broad state exemptions and the absence of explicit compensation rights weaken the Act's enforcement potential compared to the GDPR.

For biometric data and FRT specifically, EU supervisory authorities have conducted investigations, issued guidance, and imposed restrictions on unlawful deployments. In India, enforcement of biometric data protections has been limited and fragmented across sectoral regulators, with uncertain prospects for comprehensive oversight under the DPDP Act.

6.6 Scholarly Perspectives and Technical Challenges

Human Rights and Ethical Concerns:

Scholars and civil society organizations have raised fundamental concerns about FRT and biometric surveillance:

- **Discrimination and Bias:** FRT systems have demonstrated higher error rates for certain demographic groups (women, people of colour, children, elderly individuals), leading to discriminatory outcomes and wrongful identifications. These biases reflect training data imbalances and algorithmic limitations (Sharma & Sharma, 2024).
- **Chilling Effects:** Mass biometric surveillance can deter legitimate public activities (protests, political expression, religious practice) by creating a perception of constant monitoring. This chilling effect threatens democratic freedoms and civil liberties (Y. Gupta, 2025).
- **Function Creep:** Biometric systems deployed for limited purposes (e.g., border control, criminal investigation) may be expanded to broader surveillance applications without adequate public debate or legal authorization (Y. Gupta, 2025).
- **Irreversibility:** Unlike passwords or tokens, biometric identifiers cannot be changed if compromised. Data breaches involving biometric databases create permanent privacy risks (Sharma & Sharma, 2024).

Technical and Operational Challenges:

Implementing effective regulation of biometric data and FRT faces several technical challenges:

- **Accuracy and Error Rates:** FRT systems are probabilistic and subject to false positives (incorrect matches) and false negatives (missed matches). Error rates vary with demographic characteristics, image quality, and environmental conditions. Regulators must balance accuracy requirements against operational feasibility.
- **DPIA Complexity:** Conducting meaningful DPIAs for complex FRT systems requires technical expertise, access to system documentation, and understanding of algorithmic decision-making processes. Many controllers lack the capacity or incentive to conduct rigorous assessments.
- **Data Minimization vs. Utility:** Biometric systems require sufficient data quality and quantity to function effectively, creating tension with data minimization principles. Techniques like pseudonymization may reduce utility or introduce new risks.
- **Re-identification Risks:** Even anonymized or aggregated biometric data may be re-identifiable through linkage attacks or inference. The line between identifiable and anonymous biometric data is increasingly blurred.

Governance Beyond Individual Rights:

As discussed in earlier sections, scholars argue that individual rights (consent, access, erasure) are insufficient to address the systemic risks of biometric surveillance. Proposed governance mechanisms include:

- **Algorithmic Auditing:** Independent technical audits of FRT systems to assess accuracy, bias, and compliance with legal requirements.
- **Public Participation:** Involving affected communities and civil society in decisions about FRT deployment, rather than relying solely on controller assessments.
- **Sector-Specific Regulation:** Tailored rules for high-risk applications (e.g., law enforcement, border control, workplace surveillance) that reflect domain-specific values and risks.
- **Moratoria and Bans:** Temporary or permanent prohibitions on certain FRT uses (e.g., real-time mass surveillance) pending development of adequate safeguards and governance mechanisms.

6.7 Practical Implementation and Cross-Border Implications

Implementation Hurdles:

Both the EU and India face significant challenges in implementing biometric data protections:

- **Technical Capacity:** Regulators, supervisory authorities, and courts often lack the technical expertise to assess complex biometric systems, conduct meaningful oversight, and enforce requirements effectively.
- **Resource Constraints:** Even well-designed regulatory frameworks require adequate resources for supervision, investigation, and enforcement. Both jurisdictions face resource limitations that constrain oversight (Jain, 2022).

- **Political Will:** Biometric surveillance systems often serve government interests (law enforcement, national security, service delivery), creating political barriers to effective regulation and enforcement.
- **Coordination Challenges:** In India, the interaction between the DPDP Act, Aadhaar Act, sectoral regulations, and state-level rules creates coordination challenges and regulatory gaps. In the EU, coordination across member states and between supervisory authorities is essential but imperfect.

Cross-Border Data Flows and Adequacy:

The divergence between EU and Indian biometric data protections has significant implications for cross-border data flows:

- **EU Adequacy Assessment:** India's DPDP Act is unlikely to receive an EU adequacy decision in its current form, due to concerns about state exemptions, enforcement infrastructure, and deviations from GDPR standards.
- **Alternative Transfer Mechanisms:** In the absence of adequacy, transfers of biometric data from the EU to India must rely on SCCs, BCRs, or other safeguards. The *Schrems II* decision requires case-by-case assessment of the destination country's surveillance laws and enforcement capabilities, raising challenges for EU-India biometric data transfers (Jain, 2022).
- **Practical Implications:** Multinational organizations developing biometric AI systems (e.g., facial recognition, voice authentication) must navigate divergent regulatory requirements, obtain multiple consents or lawful bases, and implement jurisdiction-specific safeguards. This complexity increases compliance costs and may deter certain cross-border biometric applications.

Harmonization Prospects:

Despite differences, there are prospects for convergence:

- **Shared Principles:** Both the EU and India recognize biometric data as sensitive and requiring enhanced protection in principle. Both frameworks emphasize purpose limitation, data minimization, and individual rights.
- **International Standards:** Emerging international standards (e.g., ISO/IEC standards for biometric data protection, IEEE ethical AI standards) may provide common reference points for harmonization.
- **Practical Cooperation:** Supervisory authorities and regulators in both jurisdictions can share best practices, coordinate enforcement, and develop common approaches to novel biometric technologies.

However, fundamental divergences—particularly India's broad state exemptions and the EU's emphasis on independent oversight and judicial review—create structural barriers to full harmonization.

7. CONCLUSION

The comparative analysis of EU and Indian regulatory frameworks for privacy and data protection in AI reveals both convergence and divergence. Both jurisdictions recognize privacy as a fundamental right and have established comprehensive data protection regimes that address AI surveillance, consent in ML systems, and biometric data protection. The EU's GDPR and India's DPDP Act 2023 share core principles: lawfulness, purpose limitation, data minimization, transparency, and individual rights.

However, significant differences persist. The EU's framework is more mature, with established supervisory authorities, detailed procedural requirements (especially DPIAs), and strong enforcement mechanisms. The GDPR's treatment of biometric data as special category data, its stringent consent requirements, and its constraints on government surveillance reflect a rights-based approach that prioritizes individual autonomy and judicial oversight.

India's DPDP Act represents a hybrid approach that incorporates EU-inspired principles while accommodating developmental priorities and state interests. The Act's broad exemptions for government processing, its nascent enforcement infrastructure, and its deferred implementation details create uncertainty about practical protection levels. The unique context of Aadhaar and widespread FRT deployment further distinguishes India's regulatory landscape.

For AI surveillance and the right to privacy, the key divergence lies in the treatment of state surveillance: the EU imposes meaningful constraints through DPIAs, supervisory oversight, and judicial review, while India's state exemptions significantly limit the DPDP Act's application to government activities (Y. Gupta, 2025).

For consent and data ownership in ML systems, both jurisdictions grapple with the practical challenges of obtaining meaningful consent for large-scale, complex AI processing. The GDPR provides alternative lawful bases and emphasizes rights-based governance beyond consent, while India's framework awaits clarification through subordinate rules.

For biometric data and facial recognition, the EU's classification of biometric data as special category data and its proposed AI Act restrictions on real-time FRT contrast with India's more permissive approach and limited regulatory constraints on government deployments.

The implications for cross-border data flows, multinational AI development, and global AI governance are significant. India's DPDP Act is unlikely to receive EU adequacy, necessitating alternative transfer mechanisms and increasing compliance complexity. However, shared principles and international standards offer prospects for practical cooperation and gradual convergence.

As AI technologies continue to evolve, both jurisdictions face the challenge of adapting their frameworks to address emerging risks—from generative AI and deepfakes to emotion recognition and predictive analytics. The effectiveness of their regulatory

approaches will depend not only on statutory provisions but on enforcement capacity, technical expertise, political will, and the ability to balance innovation with fundamental rights.

REFERENCES

1) Arora, A. (2025). Constitutional protection of Personality Rights In The Era of Artificial Intelligence: A Comparative Study Of India, EU And The US. International Journal for Multidisciplinary Research, 7(4). https://doi.org/10.36948/ijfmr.2025.v07i04.53264
2) Basu, N., & Dave, R. (2025). Comparative Analysis of Laws in AI. Journal of Lifestyle and SDGs Review, 5(3), e05575. https://doi.org/10.47172/2965730X.SDGsReview.v5.n03.pe05575
3) Biju, P. R., & Gayathri, O. (2024). Algorithmic solutions, subjectivity and decision errors: a study of AI accountability. Digital Policy, Regulation and Governance, 27(5), 523–552. https://doi.org/10.1108/dprg-05-2024-0090
4) Bose, J. (2025). Artificial Intelligence in Financial Services: Navigating Legal Frameworks in India and International Jurisdictions. https://doi.org/10.31219/osf.io/2my9a_v1
5) Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. Frontiers in Human Dynamics, 6. https://doi.org/10.3389/fhumd.2024.1421273
6) Chopra, P. (2024). Ethical Implications of AI in Financial Services: Bias, Transparency, and Accountability. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 10(5), 306–314. https://doi.org/10.32628/cseit241051017
7) Cornelius, S. (2025). A Comparative Perspective on the Future of Law in a Time of Artificial Intelligence. Legal Issues in the Digital Age, 6(1), 4–27. https://doi.org/10.17323/2713-2749.2025.1.4.27
8) Determann, L., & Gupta, C. (2020). India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2019. Berkeley Journal of International Law, 37(3), 481. https://doi.org/10.15779/Z380K26B7F
9) Edwards, L., & Veale, M. (2017). Slave to the Algorithm? Why a Right to Explanationn is Probably Not the Remedy You are Looking for. Duke Law & Technology Review, 16(1), 18–84. https://doi.org/10.31228/osf.io/97upg
10) Finch, W. W., & Butt, M. (2025). Gaps in AI-Compliant Complementary Governance Frameworks' Suitability (for Low-Capacity Actors), and Structural Asymmetries (in the Compliance Ecosystem)—A Review. Preprints. https://doi.org/10.20944/preprints202509.1979.v1
11) Gaho, F. (2024). Understanding the Regulation of the Use of Artificial Intelligence Under International Law. Verdict: Journal of Law Science, 3(2), 102–110. https://doi.org/10.59011/vjlaws.3.2.2024.102-110
12) General Data Protection Regulation (EU) 2016/679. (2016). EUR-Lex
13) Gupta, S. (2025). Artificial intelligence and competition law in india: A legal response to algorithmic market collusions. European Economic Letters (EEL), 15(3), 586–609. https://doi.org/10.52783/eel.v15i3.3450
14) Gupta, Y. (2025). Facial Recognition Technology and Fundamental Right to Privacy. Social Science Research Network Electronic Journal. https://doi.org/10.2139/ssrn.5228551
15) Jain, C. (2022). Virtual Fitting Rooms: A Review of Underlying Artificial Intelligence Technologies, Current Developments, and the Biometric Privacy Laws in the US, EU and India. Social Science Research Network Electronic Journal. https://doi.org/10.2139/ssrn.4120946
16) Kaur, T., & Singh, J. (2025). Regulating AI in India: A Comparative Analysis with International Standards. Economic Sciences, 21(1), 595–601. https://doi.org/10.69889/ksaa2139
17) Kishwar, S. D., Tripathi, A., Khatoon, S., Poddar, D., & Khurana, B. (2025). Regulating deep fakes and synthetic media: Privacy, policy and global regulatory challenges. Journal of Data Protection & Privacy, 8(1), 78–96. https://doi.org/10.69554/hbgg8150
18) Manchev, A. (2024). World's First Law for Artificial Intelligence. Legal, Ethical and Economic Aspects. Education and Technologies Journal, 15(1), 225–228. https://doi.org/10.26883/2010.241.5985
19) Matai, P. (2024). Comprehensive Guide to AI Regulations: Analyzing the EU AI Act and Global Initiatives. International Journal of Computing and Engineering, 6(1), 45–54. https://doi.org/10.47941/ijce.2110
20) Nannini, L. (2024). Habemus a Right to an Explanation: so What? – A Framework on Transparency-Explainability Functionality and Tensions in the EU AI Act. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 7(1), 1023–1035. https://doi.org/10.1609/aies.v7i1.31700.
21) Nuenen, T. van, Aran, X. F., Such, J. M., & Coté, M. (2020). Transparency for whom? Assessing discriminatory AI. Computer, KCL, 53(11), 36–44. https://doi.org/10.1109/MC.2020.3002181
22) Oguntibeju, O. O. (2024). Mitigating Artificial Intelligence Bias in Financial Systems: A Comparative Analysis of Debiasing Techniques. Asian Journal of Research in Computer Science, 17(12), 165–178. https://doi.org/10.9734/ajrcos/2024/v17i12536

23) Olariu, O., & Zeleznikow, J. (2025). Human Rights-Compliant Artificial Intelligence: Regulatory Frameworks for Upholding Democracy and the Rule of Law in the Digital Age. In Digitalization and Artificial Intelligence in Courts: Opportunities and Challenges (pp. 275–297). Oxford University Press, 2025. https://doi.org/10.1093/9780198918752.003.0014
24) Raghuvanshi, C., Shukla, R., & Shukla, S. (2025). E-Governance and Ethical AI: Balancing Automation, Privacy, and Human Rights. In D. Mishra, R. Kumar, & A. B. B. A. Hamid (Eds.), Startup-driven E-government: Digital Innovation for Sustainable Ecosystems (pp. 373–388). Information Science Reference. https://doi.org/10.4018/979-8-3373-0817-3.ch014.
25) Salaria, R., Kaur, P., & Schwab, K. (2025). AI and Law: Mitigating Bias in AI through Indian Laws. International Journal of Business and Management Invention, 14(8), 06-10. https://doi.org/10.35629/8028-14080610
26) Saxena, A. K. (2024). AI in Governance and Policy Making. International Journal of Science and Research (IJSR), 13(5), 1218–1223. https://doi.org/10.21275/sr24519015426
27) Sharma, A. K., & Sharma, R. (2024). Comparative Analysis of Data Protection Laws and AI Privacy Risks in BRICS Nations: A Comprehensive Examination. Global Journal of Comparative Law, 13(1), 56–85. https://doi.org/10.1163/2211906X-13010003
28) Singh, A. K. (2025). Convergence of Artificial Intelligence and Privacy Rights in India Legal Framework. International Journal for Multidisciplinary Research, 7(4). https://doi.org/10.36948/ijfmr.2025.v07i04.52112
29) Singh, R., & Arora, N. (2025). AI, Law, and Human Rights in India: Navigating the Legal and Ethical Frontier. Journal of Information Systems Engineering and Management, 10(35s), 1021–1024. https://doi.org/10.52783/jisem.v10i35s.6182
30) Sriram, G., Sarah, J. J., & Vahini, J. B. R. (2024). Ethical Imperatives and Technical Realities: Implementing the Right to be Forgotten in Artificial Intelligence. International Research Journal on Advanced Engineering and Management (IRJAEM), 2(12), 3479–3488. https://doi.org/10.47392/irjaem.2024.0514
31) Sun, N., Miao, Y., Jiang, H., Ding, M., & Zhang, J. (2024). From Principles to Practice: A Deep Dive into AI Ethics and Regulations. ArXiv (Cornell University). https://doi.org/10.48550/arxiv.2412.04683
32) Tang, Y. (2025). Comparative frameworks for AI legislation: Policy versus market-driven models. Journal of Computational Methods in Sciences and Engineering. https://doi.org/10.1177/14727978251364480
33) The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)
34) Yadav, M., & Sharma, A. (2025). Indian Privacy Laws and the Need for Reform in light of Artificial Intelligence. International Journal of Social Science Research (IJSSR), 2(3), 42–55. https://doi.org/10.70558/ijssr.2025.v2.i3.30364