International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

Safeguarding Personal Data in AI-Powered Technologies: A Legal and Policy Analysis

Ruby Agarwal[1], Prof. Kalpana Devi[2]

Research Scholar, Faculty of Legal Studies, HRIT University, Ghaziabad 2010031

Dean, Faculty of Legal Studies, HRIT University, Ghaziabad 2010032

ABSTRACT

The rapid proliferation of Artificial Intelligence (AI)-powered technologies has fundamentally transformed the manner in which personal data is collected, processed, and utilised, raising acute questions of legal accountability and individual rights. This paper undertakes a doctrinal and comparative legal analysis of the frameworks governing personal data protection in AI-driven ecosystems, with particular reference to the General Data Protection Regulation (GDPR), India's Digital Personal Data Protection Act, 2023, and the EU Artificial Intelligence Act, 2024. The objectives are to evaluate the adequacy of existing legal regimes and to identify regulatory lacunae specific to AI-driven data processing. Employing a doctrinal and comparative methodology, the paper analyses judicial pronouncements, legislative instruments, and institutional guidelines. The analysis reveals structural inadequacies in consent-based frameworks, persistent gaps in algorithmic accountability, and enforcement asymmetries across jurisdictions. The paper concludes by recommending a risk-tiered regulatory model, codification of algorithmic accountability, and binding international cooperation to ensure meaningful protection of personal data rights in the evolving AI landscape.

Keywords: *Artificial Intelligence, Personal Data Protection, GDPR, Digital Personal Data Protection Act 2023, Algorithmic Accountability*

I. INTRODUCTION

The emergence of Artificial Intelligence as a dominant technological paradigm has precipitated an unprecedented transformation in the collection, aggregation, profiling, and automated analysis of personal data. AI-powered systems encompassing facial recognition platforms, predictive analytics engines, recommendation algorithms, credit scoring models, and large language models operate on vast datasets that invariably include sensitive personal information pertaining to identifiable individuals. This capacity for large-scale, opaque, and adaptive data processing raises profound legal questions concerning individual privacy, informational self-determination, the adequacy of existing consent mechanisms, and the institutional competence of regulatory authorities. The right to privacy is recognised as a fundamental human right under Article 12 of the Universal Declaration of Human Rights, 1948, which enjoins that no person shall be subjected to arbitrary interference with their privacy.[1] In India, this right acquired constitutional status through the unanimous nine-judge bench decision of the Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India,*[2] wherein the Court held that the right to privacy is an intrinsic component of the right

[1] Universal Declaration of Human Rights, G.A. Res. 217A, Art. 12, U.N. Doc. A/810 (Dec. 10, 1948).

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

to life and personal liberty guaranteed under Article 21 of the Constitution of India, and that informational privacy forms a distinct and enforceable facet thereof.

At the supranational level, the enactment of the General Data Protection Regulation (GDPR) by the European Parliament and the Council in 2016,[3] rendered operative from 25 May 2018, constituted a watershed development in the global evolution of data protection law. The GDPR established a comprehensive rights-based framework premised upon principles of data minimisation, purpose limitation, storage limitation, and accountability, all of which bear direct and complex application to AI-driven data processing activities.[4] India's legislative response materialised in the form of the Digital Personal Data Protection Act, 2023 (hereinafter the DPDP Act),[5] which introduced a structured framework governing the processing of digital personal data by Data Fiduciaries, though with notable omissions pertaining to AI-specific obligations. The intersection of AI and data protection, however, presents regulatory challenges that transcend the conventional doctrinal scope of privacy law. Automated decision-making systems may produce discriminatory and legally consequential outcomes; algorithmic opacity impedes the exercise of meaningful consent and the right to explanation; and the inherently transnational character of AI deployment renders unilateral jurisdictional enforcement structurally inadequate. The recently adopted EU Artificial Intelligence Act, 2024[6] represents the world's first comprehensive legally binding framework specifically governing AI systems, introducing a risk-based classificatory architecture. The OECD Principles on Artificial Intelligence, adopted in 2019,[7] further provide normative international guidance on trustworthy AI development, encompassing transparency, accountability, and the rule of law.

This paper proceeds as follows: Part II sets out the objectives; Part III delineates the methodology; Part IV analyses the definitional and principled framework governing personal data in the AI context; Part V examines the adequacy of consent; Part VI addresses cross-border data flows; Part VII analyses enforcement frameworks; Part VIII evaluates the EU AI Act as a governance model; Part IX presents findings and discussion; Part X proposes recommendations; and Part XI concludes.

II. OBJECTIVES

1. To critically analyse the existing domestic and international legal frameworks governing the protection of personal data in the context of AI-powered technologies, with particular reference to the GDPR, the Digital Personal Data Protection Act, 2023, and the EU AI Act, 2024.
2. To identify structural regulatory gaps and enforcement asymmetries in the current legal regime and to propose a harmonised, risk-tiered, and accountability-driven policy framework that adequately addresses the juridical complexities of AI-driven personal data processing.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [General Data Protection Regulation], OJ L 119, 4.5.2016, p. 1.

[4] GDPR, Art. 5(1)(a)–(f) and Art. 5(2).

[5] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023) (India), received Presidential assent on 11 August 2023.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [Artificial Intelligence Act], OJ L, 12.7.2024

[7] OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (adopted 22 May 2019).

III. METHODOLOGY

This paper adopts a doctrinal legal research methodology, grounded in the systematic analysis of primary legal sources including statutes, constitutional provisions, judicial decisions, international conventions, and official regulatory guidelines. This is supplemented by a comparative legal method, juxtaposing the regulatory architectures of the European Union, the United States of America, and the Republic of India to identify convergences, divergences, and instructive best practices. Secondary sources comprising peer-reviewed legal scholarship, institutional policy reports, and parliamentary materials are also utilised. All sources relied upon are publicly available, verified, and authentic legal instruments or authoritative institutional publications.

IV. PERSONAL DATA AND AI: THE LEGAL FRAMEWORK

A. Definitional Scope

Under Article 4(1) of the GDPR, "personal data" is defined as any information relating to an identified or identifiable natural person.[8] This definition is deliberately broad, encompassing not merely direct identifiers such as names and national identification numbers, but also indirect identifiers including IP addresses, location data, biometric data, and online behavioural identifiers all of which constitute the foundational inputs for most contemporary AI systems. The DPDP Act, 2023 defines "personal data" under Section 2(t) as any data about an individual who is identifiable by or in relation to such data,[9] reflecting a similarly expansive legislative intent. A critical legal challenge arises from the phenomenon of re-identification: data that has been anonymised may be reconstructed through the combination of multiple individually innocuous data points by machine learning algorithms. This renders conventional anonymisation an insufficiently reliable legal safeguard for compliance purposes under both instruments.

B. Foundational Principles and Their Application to AI Systems

The GDPR enshrines seven foundational principles under Article 5(1), including lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and, by virtue of Article 5(2), accountability.[10] Each of these principles presents distinctive doctrinal challenges when applied to AI systems. Purpose Limitation requires that data collected for one specified, explicit, and legitimate purpose not be processed in a manner incompatible with that purpose. AI models are, however, frequently trained on repurposed or aggregated datasets whose original collection purposes may be materially different from the downstream AI application. Regulatory bodies in the EU have increasingly scrutinised such repurposing as a potential GDPR violation.

Data Minimisation demands that only data strictly necessary for the specified purpose be collected and processed. This principle is structurally in tension with the computational requirements of large-scale AI model training, which demands vast quantities of diverse training data to achieve statistical accuracy and generalisability. Transparency obliges data controllers to provide intelligible and accessible information to data subjects regarding the nature and logic of processing operations. Algorithmic opacity colloquially referred to as the "black box" problem

[8] GDPR, Art. 4(1)

[9] The Digital Personal Data Protection Act, 2023, Section 2(t) (India).

[10] GDPR, Art. 5(1)(a)–(f) and Art. 5(2)

fundamentally undermines this obligation, as even technically expert developers may be unable to provide a sufficiently intelligible explanation of the inferential logic underlying a particular AI-generated output or decision.[11]

C. Automated Decision-Making and Profiling

Article 22(1) of the GDPR expressly confers upon data subjects the right not to be subjected to a decision based solely on automated processing including profiling which produces legal or similarly significant effects concerning them.[12] This provision is of central legal importance in the AI context, where credit scoring, insurance risk assessment, hiring decisions, benefit eligibility determinations, and criminal recidivism predictions are increasingly delegated to automated systems with minimal or no meaningful human oversight. The EU AI Act, 2024 reinforces these protections by designating AI systems deployed in high-risk domains including law enforcement, employment, education, credit scoring, and the administration of justice as "high-risk AI systems," subject to stringent pre-market obligations.[13] Article 9(1) of the EU AI Act mandates that providers of high-risk AI systems establish, implement, document, and maintain a comprehensive risk management system throughout the entire lifecycle of the system.[14]

In India, the DPDP Act, 2023, while constituting a significant legislative step, does not contain any provision directly analogous to Article 22 of the GDPR. Section 4(1) of the Act imposes a general obligation on Data Fiduciaries to process personal data only for a lawful purpose and only to the extent necessary for such purpose.[15] The conspicuous absence of explicit algorithmic accountability provisions, including any right to explanation or to contest automated decisions, constitutes a material legislative lacuna requiring remedial action.

V. CONSENT IN THE AI ECOSYSTEM: ADEQUACY AND LEGAL CRITIQUE

A. The Consent Paradigm

Consent occupies a foundational position in data protection law across all major jurisdictions. Article 6(1)(a) of the GDPR requires that processing be based on consent which is freely given, specific, informed, and unambiguous, as indicated by a clear affirmative act. The DPDP Act, 2023 similarly mandates under Section 6(1) that consent be free, specific, informed, unconditional, and unambiguous, with the additional requirement that it be accompanied by a notice in clear and plain language.[16] In the United States, the California Consumer Privacy Act, 2018 (CCPA)[17] and its successor, the California Privacy Rights Act, 2020 (CPRA),[18] provide consumers with rights to opt out of the sale and sharing of personal information, constituting the most comprehensive state-level consent protections in the US federal system.

[11] European Data Protection Board, Guidelines 02/2022 on the Application of Article 60 GDPR, adopted 14 March 2023, at para. 12

[12] GDPR, Art. 22(1).

[13] EU AI Act, 2024, Arts. 6 and 10 (classification and obligations for high-risk AI systems).

[14] EU AI Act, 2024, Art. 9(1).

[15] The Digital Personal Data Protection Act, 2023, Section 4(1) (India)

[16] The Digital Personal Data Protection Act, 2023, Section 6(1) (India).

[17] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (West 2018).

[18] California Privacy Rights Act of 2020 (Proposition 24), amending and expanding the CCPA, operative January 1, 2023.

B. Structural Inadequacies of Consent in AI Contexts

The consent model, designed for relatively linear and predictable data processing relationships, demonstrates three structural inadequacies in the AI ecosystem that the current legal architecture does not adequately resolve. First, informational asymmetry between AI developers and individual data subjects renders genuinely informed consent practically illusory in most AI-mediated interactions. A user purporting to consent to the terms of a smart voice assistant service cannot meaningfully appreciate the full scope of inferences psychological profiles, financial risk scores, health predictions that may be algorithmically derived from their vocal patterns, usage habits, and behavioural metadata.

Second, consent fatigue arising from the proliferation of lengthy, standardised privacy notices and cookie consent interfaces has been empirically documented to produce reflexive and nominal assent rather than genuine autonomous choice. The European Data Protection Board has authoritatively affirmed that consent cannot be regarded as valid where data subjects have no real choice or where refusal to consent would result in significant detriment to the individual.[19]

Third, dynamic and iterative AI processing, in which models continuously adapt and derive new inferences as additional data is ingested, means that the purpose of processing at the time of initial consent may evolve materially and unpredictably, rendering static, point-in-time consent mechanisms functionally inadequate as a continuing legal basis for AI-driven data operations.

VI. CROSS-BORDER DATA FLOWS AND JURISDICTIONAL CHALLENGES

AI-powered technologies are inherently transnational in their operational architecture, with personal data routinely traversing multiple sovereign jurisdictions during collection, storage, model training, and inference stages. This transnationality generates complex and often unresolved conflicts of law. Chapter V of the GDPR (Articles 44–49) restricts the transfer of personal data to third countries unless an adequate level of protection is ensured, either through an adequacy decision of the European Commission, standard contractual clauses, binding corporate rules, or other approved transfer mechanisms. The progressive restriction of transfer mechanisms following judicial scrutiny by EU courts has demonstrated the legal fragility of international data governance arrangements in the face of divergent national security and surveillance laws. The DPDP Act, 2023 empowers the Central Government under Section 16 to restrict cross-border transfers of personal data to specified countries or territories by way of notification, adopting a "negative list" model rather than an EU-style adequacy assessment framework. This fundamental divergence in regulatory philosophy between rights-based adequacy assessment and executive-discretionary restriction complicates compliance architecture for multinational AI developers who must simultaneously navigate both regimes. The OECD AI Policy Observatory has documented that regulatory fragmentation across jurisdictions imposes significant compliance costs on AI developers and may incentivise regulatory arbitrage the structuring of AI system

[19] European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679, adopted 4 May 2020, at p. 6.

development and deployment from jurisdictions offering comparatively weaker data protection standards.[20]

VII. ENFORCEMENT FRAMEWORKS: A COMPARATIVE ANALYSIS

A. European Union

The GDPR's enforcement architecture is, by global standards, the most structurally rigorous currently in force. Article 83(5) authorises national supervisory authorities to impose administrative fines of up to €20 million, or in the case of an undertaking, up to 4% of total worldwide annual turnover of the preceding financial year, whichever is the higher figure.[21] This turnover-linked formula is specifically designed to ensure deterrent effect against large technology corporations for whom absolute monetary maxima would be financially immaterial.

B. India

The DPDP Act, 2023 establishes the Data Protection Board of India as the principal adjudicatory authority for data protection violations. The Schedule to the Act prescribes financial penalties of up to ₹250 crore for a single instance of non-compliance with the Act's provisions, and up to ₹200 crore for failure to implement reasonable security safeguards resulting in a personal data breach.[22] While these figures are substantial in absolute terms, the absence of a turnover-linked formula substantially reduces the deterrent effect as against large multinational technology enterprises, for which absolute penalties of this quantum represent a negligible fraction of annual revenues.

C. United States

The United States continues to lack a comprehensive omnibus federal data protection statute applicable to private sector entities. Enforcement is principally undertaken by the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices in or affecting commerce.[23] The FTC's consent decree with Facebook, Inc. in 2019, imposing a civil penalty of USD 5 billion the largest penalty in the Commission's history at that time arose from findings that Facebook had violated the terms of a 2012 consent order through its sharing of user data with Cambridge Analytica without adequate disclosure to or authority from the affected data subjects.[24] The absence of a statutory private right of action at the federal level remains a significant structural limitation on the efficacy of US data protection enforcement.

VIII. THE EU AI ACT, 2024: A RISK-TIERED GOVERNANCE MODEL

The EU Artificial Intelligence Act, 2024 establishes the world's first comprehensive, horizontally applicable, legally binding framework specifically governing the development, placement on the market, and use of AI systems in the European Union.[25] The Act adopts a four-tier risk classification architecture: (i) AI practices posing unacceptable risk, which are expressly prohibited; (ii) high-risk AI systems, subject to extensive pre-market and ongoing compliance obligations; (iii) AI systems with limited risk, subject to transparency

[20] OECD.AI Policy Observatory, *State of Implementation of the OECD AI Principles: Insights from National AI Policies* (OECD Publishing, Paris, 2021).

[21] GDPR, Art. 83(5).

[22] The Digital Personal Data Protection Act, 2023, Section 33 read with Schedule, Items 1 and 3 (India).

[23] Federal Trade Commission Act, 15 U.S.C. § 45.

[24] In the Matter of Facebook, Inc., FTC File No. 1923109, Decision and Order (Federal Trade Commission, 24 July 2019).

[25] EU AI Act, 2024, Art. 99(3) (fines for violations relating to prohibited AI practices and high-risk system obligations).

obligations; and (iv) AI systems posing minimal risk, which remain unregulated. Prohibited AI practices under the Act include the use of subliminal techniques to manipulate individual behaviour, exploitation of vulnerabilities of specific groups, biometric categorisation of natural persons based on sensitive attributes, and subject to narrow exceptions real-time remote biometric identification systems in publicly accessible spaces. High-risk AI systems are subject to obligations including mandatory data governance requirements, technical documentation, registration in an EU database, transparency obligations towards users, and requirements for human oversight.

Sanctions under the EU AI Act are structured on a tiered basis: violations involving prohibited AI practices attract fines of up to €35 million or 7% of global annual turnover; violations of other obligations attract fines of up to €15 million or 3% of global annual turnover; and the provision of incorrect information to authorities attracts fines of up to €7.5 million or 1.5% of global annual turnover.

IX. FINDINGS

The comparative doctrinal analysis conducted in this paper yields the following consolidated findings:

First, the GDPR and the EU AI Act together constitute the most comprehensive and mutually reinforcing data protection and AI governance regime currently in operation globally. Nevertheless, persistent gaps remain with respect to explainability requirements for general-purpose AI models, the regulation of foundation models deployed outside EU territorial jurisdiction, and the enforcement of rights against non-EU-established AI providers.

Second, India's DPDP Act, 2023, while representing a landmark legislative development, exhibits material deficiencies in its failure to provide expressly for algorithmic accountability, a right to contest automated decisions, AI-specific data governance standards, and meaningful independent oversight mechanisms for AI processing activities. The Act's structural reliance on delegated legislation introduces normative uncertainty.

Third, the United States' fragmented, sectoral, and enforcement-centred approach, while offering regulatory flexibility, lacks the systemic coherence and prescriptive rights-protection necessary to govern increasingly pervasive and consequential AI-driven data practices at scale.

Fourth, the pronounced absence of a binding international legal instrument on AI and personal data notwithstanding the existence of soft-law instruments such as the OECD AI Principles and the UNESCO Recommendation on the Ethics of AI perpetuates normative fragmentation and undermines effective global accountability.

Fifth, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, while supplementing India's existing legal framework under the Information Technology Act, 2000, are technologically dated and substantively inadequate to address the complex and evolving data security risks inherent in AI-driven processing environments.

X. CONCLUSION

The legal challenge of safeguarding personal data in AI-powered technologies represents one of the most consequential and structurally complex problems confronting contemporary legal scholarship and regulatory practice. The frameworks examined in this paper the GDPR, India's DPDP Act, 2023, the EU AI Act, 2024, and the US enforcement-based model collectively represent the current frontier of legal response to AI-driven data processing. Yet each exhibits deficiencies that reflect the fundamental reality that these instruments were designed to address data protection challenges of an earlier technological era, not the adaptive, opaque, and globally networked systems that characterise modern AI. The constitutional guarantee of the right to privacy under Article 21 of the Constitution of India, as authoritatively affirmed by the Supreme Court in *Puttaswamy*, provides a foundational juridical basis upon which a more robust and rights-protective domestic AI governance architecture can and must be constructed. The existing legislative framework, however, requires systematic recalibration through legislative amendment, delegated regulation, and judicial interpretation to give substantive legal effect to that constitutional guarantee in the AI era. Ultimately, the effective safeguarding of personal data in AI-powered technologies demands not merely reactive, incident-driven regulation, but proactive, anticipatory, and technically informed legal frameworks anchored in the constitutional values of human dignity, informational autonomy, and the rule of law

.