Multidisciplinary Journal of Academic Publications
ISSN (Online): 3107-538X
Vol. 02, Issue 02, March – April 2026

# REASSESSING PERSONAL DATA PROTECTION LAWS IN THE AGE OF ARTIFICIAL INTELLIGENCE: A CRITICAL STUDY

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

**Research Scholar, Faculty of Legal Studies, HRIT University, Ghaziabad 201003[1]**

**Dean, Faculty of Legal Studies, HRIT University, Ghaziabad 201003[2]**

## Abstract

*Artificial Intelligence has emerged as a transformative force in contemporary data-driven economies, fundamentally altering the scale, speed, and sophistication with which personal data is collected, processed, and monetised. This paper undertakes a doctrinal and comparative legal analysis of the adequacy of existing personal data protection frameworks principally India's Digital Personal Data Protection Act, 2023 and the European Union's General Data Protection Regulation, 2016 in governing AI-driven data processing. Through critical examination of the structural features of AI systems, including algorithmic opacity, automated decision-making, mass profiling, and cross-border data flows, the paper identifies systemic inadequacies in consent-based legal architectures that were substantially conceived in a pre-AI regulatory paradigm. Drawing upon landmark judicial pronouncements including Justice K.S. Puttaswamy v. Union of India, Google Spain v. AEPD, and Schrems II, as well as peer-reviewed scholarship and institutional reports, the paper demonstrates that current frameworks particularly India's DPDP Act lack enforceable protections against algorithmic discrimination, autonomous decision-making, and surveillance capitalism. The paper further undertakes a comparative evaluation of the India–EU regulatory divide, exposing gaps in India's legislative architecture including the absence of provisions equivalent to Article 22 of the GDPR. Based on this critical analysis, the paper advances concrete, non-generic reform proposals encompassing AI-specific regulatory legislation, algorithmic transparency mandates, an independent AI regulatory authority, and mandatory ethical compliance audits. The paper concludes that effective data protection in the AI era demands a fundamental reorientation from consent-centric models towards accountability-based governance frameworks that place individual fundamental rights at the normative centre of regulatory design.*

**Keywords:** *Artificial Intelligence[1], Personal Data Protection[2], Digital Personal Data Protection Act 2023[3], General Data Protection Regulation[4], Algorithmic Accountability[5].*

## 1. Introduction

The proliferation of Artificial Intelligence (AI) across sectors from healthcare diagnostics and financial credit scoring to targeted advertising and predictive policing has fundamentally altered the architecture of data-driven economies. AI systems are not self-sustaining constructs; they depend upon the continuous ingestion, processing, and analysis of vast volumes of personal data, without which the predictive and classificatory

capabilities that generate commercial and governmental value would be impossible to achieve.[1] The more data available for algorithmic training, the more refined and commercially valuable the resulting outputs become. This symbiosis between AI capability and personal data processing has produced a foundational tension: the economic imperative to innovate collides directly with the constitutional imperative to protect individual privacy.[2] The inadequacy of existing legal frameworks to govern this collision constitutes the central research problem of this paper. Personal data protection laws including India's recently enacted Digital Personal Data Protection Act, 2023 (DPDP Act) and the European Union's General Data Protection Regulation (GDPR) were substantially conceived around the paradigm of human-directed, purpose-specific data processing, not autonomous algorithmic systems operating at scale. AI's distinguishing characteristics opacity, self-learning, automated decision-making, and data intensity expose systemic gaps in consent architectures, enforcement mechanisms, and rights frameworks. Through a doctrinal and comparative analysis, this paper critically examines whether current legal regimes are adequately equipped to govern AI-driven data processing and proposes reforms calibrated to the emergent technological reality.

## 2. Conceptual Framework: AI and Personal Data Protection

Artificial Intelligence, defined by the OECD as "a machine-based system that, for a given set of objectives, makes predictions, recommendations, or decisions influencing real or virtual environments,"[3] encompasses machine learning, deep learning, natural language processing, and large language models. Machine learning the dominant paradigm in commercial AI deployment involves training algorithms on large datasets to identify patterns and generate predictions without explicit rule-based programming, rendering AI systems fundamentally distinct from conventional software in their operation and governance requirements.[4] Personal data, under Article 4(1) of the GDPR, comprises any information relating to an identified or identifiable natural person.[5] The DPDP Act, 2023 adopts a broadly comparable definition under Section 2(t), encompassing any data about an individual who is identifiable by or in relation to such data.[6] "Sensitive personal data" including health records, biometric information, financial data, and sexual orientation attracts heightened protection under Article 9 of the GDPR, reflecting the elevated potential for harm upon its misuse.[7] Profiling, operationally understood as automated processing of personal data to evaluate aspects of an individual's personality, behaviour, or preferences, is the principal mechanism through which AI converts raw data into commercially actionable outputs. The structural risks of AI-based data processing are manifold. First, AI systems embed bias from training datasets, systematically disadvantaging protected classes in high-stakes decision contexts.[8] Second, the opacity of algorithmic models the "black box" problem renders it structurally impossible for individuals to understand or meaningfully contest decisions made about them.[9] Third, AI enables mass surveillance infrastructure capable of monitoring and profiling entire populations at unprecedented scale and granularity.[10]

[1] OECD, *Artificial Intelligence in Society* (OECD Publishing 2019) 22.
[2] General Data Protection Regulation (EU) 2016/679 [hereinafter GDPR]; Digital Personal Data Protection Act 2023 (India) [hereinafter DPDP Act]
[3] OECD, 'Recommendation of the Council on Artificial Intelligence' (OECD/LEGAL/0449, 2019) para 1.1.
[4] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16(1) *Duke Law & Technology Review* 18, 21–23.
[5] GDPR art 4(1).
[6] DPDP Act 2023 (India), s 2(t).
[7] GDPR art 9(1).
[8] Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1, 4–8.
[9] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 3–18.
[10] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019) 7–11.

These risks collectively demand a legal response that significantly exceeds the scope of conventional data protection law.

## 3. Legal Frameworks Governing Data Protection

**India: DPDP Act, 2023 and IT Act, 2000**

The Digital Personal Data Protection Act, 2023 represents India's first comprehensive, cross-sectoral data protection legislation, superseding the previously fragmented protections available under Section 43A of the Information Technology Act, 2000, which had imposed compensatory liability on corporate entities for negligent handling of sensitive personal data.[11] The DPDP Act establishes a consent-based framework in which a "Data Fiduciary" any person who alone or in conjunction with others determines the purpose and means of processing personal data[12] must obtain free, specific, informed, and unambiguous consent from the "Data Principal" prior to processing.[13] The Act further recognises rights of Data Principals including rights to information, correction, erasure, and grievance redressal.[14] Critically, however, the DPDP Act contains no provision governing automated decision-making or algorithmic processing. It offers no right to human review of algorithmically generated decisions, imposes no transparency obligations on AI systems, and does not address the particular risks of profiling or AI-driven discrimination. The Srikrishna Committee's 2018 report had recommended provisions specifically addressing automated decision-making and profiling,[15] but these were substantially excised from the final legislation a decision that creates a significant governance lacuna, given that AI systems inherently and necessarily process large volumes of personal data as an operational precondition.

**European Union: GDPR and UK Data Protection Act, 2018**

The GDPR constitutes the most architecturally developed data protection instrument in the world. Its foundational principles including purpose limitation, data minimisation, storage limitation, accuracy, integrity, and accountability[16] impose substantive constraints on data processing that extend beyond the consent mechanism. The GDPR's consent model under Article 7 demands that consent be freely given, specific, informed, and unambiguous, with the evidentiary burden placed on the Data Controller to demonstrate valid consent.[17] Of paramount significance in the AI context is Article 22, which grants data subjects the right not to be subject to decisions based solely on automated processing including profiling that produce legal or similarly significant effects concerning them.[18] Recital 71 of the GDPR further mandates that data subjects retain the right to obtain human intervention, to express a point of view, and to contest automated decisions.[19] This provision constitutes the most legally developed response to algorithmic decision-making in any extant data protection framework. The UK Data Protection Act 2018, substantially retaining GDPR architecture, extends specific protections under Section 14 to solely automated decisions involving special category data.[20] Additionally, Article 25 GDPR imposes obligations of data protection by design and by default, requiring that privacy-

[11] Information Technology Act 2000 (India), s 43A; DPDP Act 2023 (India), Preamble
[12] DPDP Act 2023 (India), s 2(i).
[13] DPDP Act 2023 (India), s 6(1).
[14] DPDP Act 2023 (India), ss 11–13.
[15] Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India 2018) 43–47
[16] GDPR art 5(1)(a)–(f).
[17] GDPR art 7.
[18] GDPR art 22(1).
[19] GDPR Recital 71.
[20] UK Data Protection Act 2018, s 14(1).

protective measures be embedded into data processing systems from inception a provision with direct relevance to AI system development.[21]

## 4. Key Challenges in the Age of AI

### Consent Fatigue and the Meaningful Consent Problem

The consent model the cornerstone of both the DPDP Act and the GDPR is structurally ill-suited to AI environments. AI systems require dynamic, ongoing access to personal data across multiple contexts simultaneously, whereas consent architecture presupposes discrete, temporally bounded transactions.[22] Schwartz and Solove have persuasively argued that the concept of informed consent becomes incoherent when applied to data ecosystems where individuals cannot reasonably anticipate secondary uses of their data, particularly in machine learning contexts where training and inference involve data flows across jurisdictions and platforms.[23] The Cambridge Analytica scandal in which approximately 87 million Facebook users' data was harvested for psychographic political profiling through nominally consented third-party application permissions starkly demonstrated how consent mechanisms can be instrumentalised to legitimise large-scale data exploitation.[24]

### Algorithmic Bias and Discrimination

AI systems trained on historically biased datasets reproduce and amplify systemic discrimination. Citron and Pasquale have demonstrated how automated scoring systems deployed in credit evaluation, employment screening, and criminal risk assessment embed socioeconomic and racial disparities into decision architectures, producing outcomes that are simultaneously discriminatory and legally opaque.[25] Existing data protection frameworks address discrimination incidentally through sensitive data categorisations, but lack structural tools to mandate algorithmic auditing, bias testing, or compel remediation of discriminatory outcomes.

### The Black Box Problem

The opacity of contemporary AI architectures particularly deep learning models renders them fundamentally incompatible with the transparency and accountability norms underpinning data protection law. Pasquale's seminal analysis demonstrates how algorithmic opacity enables powerful commercial and governmental actors to make consequential decisions affecting individuals without disclosing the criteria, logic, or reasoning involved.[26] Wachter, Mittelstadt, and Floridi further argue that even the GDPR's explanation provisions, properly construed, do not extend to the systemic logic of algorithmic models, leaving affected individuals without meaningful recourse.[27]

[21] GDPR art 25.
[22] Paul M Schwartz and Daniel J Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 *New York University Law Review* 1814, 1829–1832.
[23] Neil M Richards and Jonathan H King, 'Three Paradoxes of Big Data' (2013) 66 *Stanford Law Review Online* 41, 44–46.
[24] Information Commissioner's Office (ICO), *Investigation into the Use of Data Analytics in Political Campaigns: Investigation Update* (November 2018) 4.
[25] Citron and Pasquale (n 8) 14–22.
[26] Pasquale (n 9) 25–48.
[27] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) *International Data Privacy Law* 76, 78–82.

**Mass Surveillance and Data Exploitation**

Zuboff's concept of "surveillance capitalism" identifies the structural transformation through which AI converts personal data from a byproduct of digital activity into the primary raw material for behavioural prediction markets, enabling platforms to anticipate and modify human behaviour at scale.[28] Feldstein's Carnegie Endowment research documents AI-based surveillance infrastructure deployments across 75 countries, raising acute concerns regarding accountability, legality, and democratic governance in the absence of binding international legal frameworks.[29]

**Cross-Border Data Transfers**

The Schrems II judgment invalidated the EU-US Privacy Shield, holding that US surveillance law provides inadequate protection equivalent to EU fundamental rights standards.[30] This ruling has profound operational implications for AI supply chains, which routinely involve cross-jurisdictional data flows across cloud infrastructure, training datasets, and model deployment environments. India's DPDP Act currently provides an inadequate cross-border transfer framework, relying on a government-approved "white list" mechanism that does not engage substantively with the adequacy of foreign legal protections.

## 5. Case Laws and Judicial Trends

**Justice K.S. Puttaswamy v. Union of India (2017)**

The nine-judge constitutional bench in *Puttaswamy* unanimously recognised the right to privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution of India.[31] The Court's substantive privacy jurisprudence identified informational privacy, bodily integrity, and decisional autonomy as constitutive dimensions of the right. Critically, Justice D.Y. Chandrachud's concurring judgment articulated that surveillance and data collection by the State must satisfy the requirements of legality, necessity, and proportionality a tripartite standard that directly challenges the unchecked deployment of AI-based surveillance systems by government agencies. *Puttaswamy*'s constitutional endorsement of informational self-determination implicitly mandates that AI-driven processing satisfy proportionality standards that the DPDP Act's current framework does not explicitly operationalise.

**Google Spain v. AEPD (2014)**

The Court of Justice of the European Union (CJEU) in *Google Spain* established the "right to be forgotten," holding that individuals may require search engines to delist links to outdated, irrelevant, or excessive personal information, even where that information was originally lawfully published.[32] In the AI context, this judgment raises critical questions regarding the obligations of AI operators to de-index personal data from training datasets, the feasibility and legal obligation to "unlearn" or retrain models built on unlawfully retained data, and

[28] Zuboff (n 10) 94–97.
[29] Steven Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace, Working Paper, September 2019) 3.
[30] *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Case C-311/18) [2020] ECLI:EU:C:2020:559 [*Schrems II*], paras 178–185.
[31] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1, paras 325–327 (Chandrachud J).
[32] *Google Spain SL v Agencia Española de Protección de Datos (AEPD)* (Case C-131/12) [2014] ECLI:EU:C:2014:317, paras 93–94

the territorial scope of algorithmic data removal obligations. The ruling thus extends well beyond search engine governance into the architecture of AI training and data lifecycle management.

**Data Protection Commissioner v. Facebook Ireland (Schrems II, 2020)**

The CJEU's invalidation of the EU-US Privacy Shield in *Schrems II* affirmed that adequate data protection requires not merely contractual guarantees, but substantive legal protections enforceable in practice against foreign intelligence agencies.[33] For AI systems that process European personal data on US-based infrastructure a near-universal commercial reality *Schrems II* demands robust legal mechanisms that Standard Contractual Clauses alone cannot provide, given the breadth of US intelligence community access authorisations under Section 702 FISA. The judgment underscores that data protection law must engage substantively with the geopolitical architecture of AI infrastructure deployment.

## 6. Critical Evaluation of Existing Laws

A comparative evaluation reveals significant structural divergence between the Indian and EU approaches to data protection in the AI era, with the EU framework offering considerably more developed though still imperfect governance architecture. The GDPR's strength lies in its risk-based, technology-neutral design, supplemented by detailed guidance from the Article 29 Working Party and its successor, the European Data Protection Board.[34] Article 22's automated decision-making protections, data protection impact assessment obligations, and the by-design principle collectively constitute a framework capable of partial adaptation to AI risks. Nevertheless, the GDPR exhibits limitations: Article 22 exemptions for contractual necessity and explicit consent are routinely deployed to circumvent its protections, and the right to explanation remains normatively contested and practically limited in scope.[35] India's DPDP Act presents more fundamental inadequacies in the AI context. First, there is no provision equivalent to Article 22 GDPR no right to human review of automated decisions, no obligation to explain algorithmic determinations, and no prohibition on consequential automated processing without substantive safeguards. Second, the Act's enforcement architecture vesting regulatory authority in a Data Protection Board whose members are appointed by and accountable to the Central Government raises separation of powers concerns and creates structural risks of regulatory capture.[36] Third, the consent model is not supplemented by a proportionality framework or legitimate interests basis, making the statute structurally over-reliant on consent even in contexts where meaningful consent is architecturally impossible. Richards and King have argued persuasively that data protection law's foundational categories notice, consent, and purpose specification are ill-adapted to the emergent realities of large-scale data analytics and machine intelligence.[37] This critique applies with full force to the DPDP Act, which was enacted with awareness of these limitations yet failed to address them legislatively. The CIS India analysis of data governance frameworks further cautions that regulatory regimes failing to address algorithmic accountability will become operationally irrelevant to AI governance regardless of their formal comprehensiveness.[38]

[33] *Schrems II* (n 30) paras 183–202
[34] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (WP251rev.01, 6 February 2018).
[35] Wachter, Mittelstadt and Floridi (n 27) 90–94; Edwards and Veale (n 4) 46–52.
[36] DPDP Act 2023 (India), s 18.
[37] Richards and King (n 23) 48–50.
[38] Arindrajit Basu, Elonnai Hickok and Aditya Singh Chawla, *The Localisation Gambit: Unpacking Policy Measures for Sovereignty over Data* (Centre for Internet and Society, India 2019) 12–15.

## 7. Recommendations and Reform Suggestions

The analysis above demonstrates the need for a fundamental reconceptualisation of data protection law as an instrument of AI governance. The following reforms are proposed. *First*, India requires either a dedicated AI regulatory framework or comprehensive amendment to the DPDP Act, incorporating provisions equivalent to Article 22 GDPR, including a right not to be subject to solely automated decisions producing significant effects, a right to human review, and a right to a meaningful explanation of automated determinations, calibrated to the specific risks of different AI system architectures. *Second*, algorithmic transparency mandates should be established as legal obligations for high-risk AI systems deployed in credit assessment, employment, healthcare, education, and criminal justice. Drawing upon the Article 29 Working Party's authoritative guidelines on automated decision-making,[39] transparency obligations should extend beyond mere disclosure of the existence of automated processing to encompass the logic, principal parameters, and significant consequences of algorithmic determinations. *Third*, an independent AI regulatory authority should be established, insulated from executive control, with technical expertise and enforcement powers commensurate with the scale of AI deployment in India. Regulatory independence is essential to credible enforcement against both commercial and governmental actors. *Fourth*, data minimisation principles already codified in Article 5(1)(c) of the GDPR[40] must be strengthened through mandatory prohibitions on speculative data collection for AI training, accompanied by retention limits calibrated to demonstrated operational necessity rather than commercial preference. *Fifth*, ethical AI compliance audits conducted by accredited, independent third parties should be mandated for all large-scale personal data processing systems employing AI. The OECD AI Principles provide a normative baseline for such audits,[41] and the ICO's Cambridge Analytica investigation demonstrated definitively that self-regulatory models are structurally inadequate to govern AI-driven data exploitation.[42]

## 8. Conclusion

The intersection of AI and personal data protection represents one of the most consequential legal governance challenges of the twenty-first century. Existing frameworks including both the DPDP Act, 2023 and the GDPR were designed around pre-AI paradigms of data processing and exhibit structural inadequacies when confronted with AI's defining characteristics: opacity, scale, automated decision-making, and continuous self-learning. As *Puttaswamy* affirmed, privacy is not a conditional entitlement but a fundamental constitutional guarantee, and its effective protection in the AI era demands adaptive, technologically aware, and institutionally credible legal instruments. The reform imperative is clear: consent-based models must be supplemented by accountability-based governance frameworks; algorithmic transparency must become a legal obligation rather than a commercial aspiration; and independent regulatory institutions must possess the technical capacity to enforce meaningful compliance. The challenge for legislators is not to obstruct AI innovation which offers transformative potential in healthcare, education, and economic inclusion but to ensure that such innovation does not proceed at the cost of fundamental rights. A future-ready legal framework must locate the individual, not the algorithm, at its normative centre.

[39] Article 29 Working Party (n 34) 8–12.
[40] GDPR art 5(1)(c).
[41] OECD AI Principles (n 3) Principle 1.3.
[42] ICO (n 24) 6–8.