© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1717032

Automated Profiling, Privacy Rights, and Gaps in India's DPDP Act 2023.

ABHINAV SINGH[1], DR TARU MISHRA[2]

Abstract*—The rapid proliferation of artificial intelligence and algorithmic decision-making systems in India has created an urgent need for robust legal frameworks that protect the fundamental right to privacy. The Digital Personal Data Protection Act, 2023 (DPDP Act), India's first comprehensive data protection legislation, represents a landmark legislative response to the constitutional mandate established by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). This paper examines the intersection of algorithmic decision-making, the DPDP Act, and the right to privacy in India. It critically evaluates the Act's provisions, their adequacy in addressing algorithmic harms, and the regulatory gaps that persist. The paper argues that while the DPDP Act marks an important step forward, it falls short of providing a comprehensive framework for algorithmic accountability, and that India urgently requires a dedicated AI regulatory architecture to protect citizens' fundamental rights in an increasingly automated world.

***Keywords:* Algorithmic Decision-Making, Digital Personal Data Protection Act 2023, Right to Privacy, India, Artificial Intelligence, Data Fiduciary, Significant Data Fiduciary, Puttaswamy Judgment.**

I. INTRODUCTION

India stands at a critical juncture in its digital evolution. With over 800 million internet users and one of the world's fastest-growing digital economies[1], the country has experienced an exponential expansion of data-driven technologies. Artificial intelligence systems now make consequential decisions about who receives loans, who is flagged as a security risk, who is offered employment, and who is denied government benefits. [2] These algorithmic systems, often operating as "black boxes", make determinations without transparency, without explanation, and frequently without meaningful human oversight. [3]

The question that confronts Indian constitutional law, administrative law, and the emerging data protection regime is deceptively simple but profoundly important: when an algorithm makes a decision that reshapes someone's fundamental rights, and no one can explain how it reached that conclusion, what legal recourse does the affected individual have? [4]

The enactment of the Digital Personal Data Protection Act, 2023 (hereinafter referred to as the "DPDP Act" or "the Act") marked a watershed moment in India's legal history. Receiving Presidential assent on August 11, 2023,[5] it was the culmination of a legislative journey that began in the aftermath of the Supreme Court's historic 2017 ruling in Puttaswamy v. Union of India, which recognised privacy as a fundamental right.[6] The Act introduces a comprehensive framework governing the collection, processing, storage, and transfer of digital personal data, establishing rights for individuals and obligations for entities that process their data.[7]

Yet the Act's adequacy in confronting the specific challenges posed by algorithmic decision-making remains deeply contested. This paper undertakes a rigorous analysis of the DPDP Act's provisions as they relate to algorithmic accountability, contextualised within India's constitutional framework and compared with international regulatory models. It concludes with the author's personal assessment of the Act's shortcomings and a set of reform recommendations.

II. THE CONSTITUTIONAL FOUNDATION: THE RIGHT TO PRIVACY IN INDIA

2.1 The Pre-Puttaswamy Era

Before 2017, the right to privacy in India occupied an uncertain constitutional position. The Supreme Court's decisions in M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1962) had, to varying degrees, denied or limited the existence of a fundamental right to privacy. [8] This left Indian citizens without a robust constitutional shield against state intrusion into their personal information, a gap that became increasingly untenable as India's digital economy expanded.

2.2 Justice K.S. Puttaswamy (Retd.) v. Union of India (2017): A Constitutional Watershed

On August 24, 2017, a nine-judge bench of the Supreme Court of India delivered a unanimous verdict in Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., holding that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution of India. [9] The case arose from a challenge to the Aadhaar biometric identity scheme, but its implications extended far beyond that specific controversy. [10]

The bench unanimously held that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."[11] In doing so, it explicitly overruled the prior decisions in Kharak Singh and M.P. Sharma to the extent that they had denied the constitutional status of privacy.[12]

The Court articulated privacy as encompassing three distinct dimensions: (i) privacy of the body, protecting physical integrity; (ii) informational privacy, recognising an individual's right to control the dissemination of personal information; and (iii) the privacy of choice, protecting autonomy over fundamental personal decisions.[13] Justice Chandrachud's lead opinion recognised that privacy encompasses "the body (and bodily integrity), the mind (and informational self-determination), and intimate choices," holding that all nine judges agreed that privacy was at the heart of individual self-determination, dignity, autonomy, and liberty.[14]

Critically, the Court adopted a three-pronged test for any permissible encroachment upon the right to privacy: (i) legality, the existence of a law authorising the encroachment; (ii) necessity, the pursuit of a legitimate state objective; and (iii) proportionality, a rational nexus between the means employed and the object sought.[15] This proportionality standard would later become the constitutional yardstick against which all data processing activities, including algorithmic decision-making, must be measured.

Justice Kaul, in his concurring opinion, specifically discussed the right to informational privacy and the right to preserve personal reputation, urging that "the law must provide for data protection and regulate national security exceptions that allow for interception of data by the State."[16] The Court also noted that the collection of information about a person gives power over them and that this would have a "chilling effect not only on the expression of dissent but also on the exercise of fundamental rights."[17]

The Puttaswamy judgment thus laid the constitutional groundwork for data protection legislation and, by extension, for the regulation of algorithmic systems that process personal data to make consequential decisions. [18]

2.3 Informational Self-Determination and the Algorithmic Context

The concept of informational privacy articulated in Puttaswamy, encompassing an individual's right to control the dissemination of personal information[19], has profound implications for algorithmic decision-making. When algorithms process vast quantities of personal data to generate profiles, predictions, and automated decisions, they implicate the informational privacy of every data subject. The Puttaswamy framework demands that such processing be lawful, necessary, and proportionate, standards that many current algorithmic deployments in India demonstrably fail to meet. [20]

III. THE LEGISLATIVE JOURNEY TO THE DPDP ACT, 2023

3.1 From Puttaswamy to Legislation

The Puttaswamy verdict directly catalysed the process of formulating a comprehensive data protection framework for India. [21] The Court commended to the Union Government "the need to examine and put into place a robust regime for data protection," cautioning that such a regime requires "a careful and sensitive balance between individual interests and legitimate concerns of the state."[22]

In December 2018, the Government constituted a committee of experts under the chairmanship of Justice B.N. Srikrishna to deliberate on a data protection framework for India. [23] The committee's report and a draft Personal Data Protection Bill were released in 2018, followed by a revised Bill in 2019 that was eventually withdrawn in 2022 because it had become unwieldy with amendments. [24]

3.2 The 2022 Consultation and the 2023 Act

On November 18, 2022, the Ministry of Electronics and Information Technology (MeitY) released the Digital Personal Data Protection Bill, 2022, for

public consultation.[25] After extensive deliberation, the Cabinet approved the revised Digital Personal Data Protection Bill, 2023, on July 5, 2023.[26] The Bill passed both Houses of Parliament in August 2023 and received Presidential assent on August 11, 2023, becoming the Digital Personal Data Protection Act, 2023.[27]

India thereby became the 19th country among the G20 members to pass a comprehensive personal data protection law. [28]

3.3 The DPDP Rules, 2025

On November 13, 2025, MeitY notified the Digital Personal Data Protection Rules, 2025 (DPDP Rules), which operationalise the DPDP Act.[29] The Rules are being implemented in a phased manner, with full compliance expected by May 13, 2027.[30] Until the core operational provisions of the Act come fully into force, the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 continue to govern the privacy regime in India.[31]

IV. KEY PROVISIONS OF THE DPDP ACT, 2023

4.1 Scope and Application

The DPDP Act pertains to the processing of digital personal data within India, encompassing situations where personal data is either collected in digital form or collected in non-digitised form and subsequently converted into digital form.[32] It also has extra-territorial applicability, applying to foreign entities that offer goods and services to Data Principals located within India.[33] Importantly, the Act applies only to personal data in digital form and does not regulate non-personal and non-digital data.[34]

4.2 Key Definitions and Actors

The Act defines ‘personal data’ broadly to include "any data about an individual who is identifiable by or in relation to such data."[35] It establishes a framework built around three principal actors:

- Data Principal: The individual to whom the personal data relates.
- Data Fiduciary: Any person who, alone or with others, determines the purpose and means of processing personal data. [36]
- Data Processor: Any person who processes personal data on behalf of a Data Fiduciary.

Notably and in contrast to other international data protection frameworks, the DPDP Act treats all personal data uniformly, without imposing heightened obligations for sensitive personal data. [37] This is a significant departure from the GDPR model and has attracted considerable criticism from privacy advocates.

4.3 Consent as the Cornerstone

The Act makes consent the cornerstone of data processing.[38] Personal data may be processed only for a lawful purpose upon consent of an individual, and consent must be free, specific, informed, unconditional, and unambiguous.[39] Consent may not be required for specified legitimate uses such as voluntary sharing of data by the individual or processing by the State for permits, licenses, benefits, and services.[40]

Every request for consent must be presented to the Data Principal in clear and plain language, providing the option to access such request in English or any language specified in the Eighth Schedule to the Constitution. [41] Data Principals can withdraw consent at any time, and the process must be as easy as giving consent. [42]

4.4 Rights of Data Principals

The Act grants certain rights to individuals, including: (i) the right to obtain information about processing; (ii) the right to seek correction and erasure of personal data; (iii) the right to grievance redressal; and (iv) the right to nominate a representative in case of incapacity. [43]

4.5 Obligations of Data Fiduciaries

Data Fiduciaries are obligated to maintain the accuracy of data, keep data secure, and delete data once its purpose has been met. [44] The Act mandates that Data Fiduciaries implement reasonable security safeguards to prevent personal data breaches and notify the Data Protection Board and affected Data Principals in the event of a breach. [45]

4.6 Data Protection Board of India

The central government will establish the Data Protection Board of India, a body corporate with powers to monitor compliance, impose penalties, direct Data Fiduciaries to take necessary measures in the event of a data breach, and hear grievances made by affected persons.[46] However, the Board does not have the power to pass regulations; the Government

is conferred broad discretion in adopting delegated legislation to further specify the provisions of the Act.[47]

4.7 Penalties

Non-compliance with the DPDP Act can lead to significant financial penalties. The maximum penalty is Rs. 250 crores for failure to take reasonable security safeguards resulting in a data breach. [48] Processing children's data in violation of the Act attracts up to Rs. 200 crores. [49] Failure to notify the Data Protection Board and affected Data Principals in the event of a personal data breach is also penalised up to Rs. 200 crores. [50]

4.8 Government Exemptions

A significant and controversial feature of the Act is the broad exemptions granted to government bodies. The Act grants wide exemptions to government entities for activities related to national security, public order, foreign relations, and crime prevention. [51] These broad exemptions have been criticised as potentially subverting the right to privacy and enabling mass surveillance without adequate safeguards. [52]

V. ALGORITHMIC DECISION-MAKING: CONCEPTUAL FRAMEWORK AND LEGAL CHALLENGES

5.1 What is Algorithmic Decision-Making?

Algorithmic decision-making refers to the use of computational systems, including machine learning models, predictive analytics, and automated rule-based systems, to make or significantly influence decisions that affect individuals. AI systems operate by learning from vast amounts of data, identifying patterns, and making decisions that improve through continuous data processing.[53] In India, artificial intelligence systems increasingly determine who receives loans, benefits, or police attention.[54]

5.2 The "Black Box" Problem

AI differs from traditional technology in that it comprises self-learning models, which often act as "black boxes," reaching conclusions without transparency on how they did so.[55] This opacity makes attributing legal liability in instances of damage much more complex.[56] When government agencies use AI systems to make determinations about bail, employment, or welfare access, individuals have a constitutional right derived from Puttaswamy and natural justice principles to understand the basis for those decisions.[57] Current AI systems, operating as black boxes, systematically violate this principle.[58]

5.3 Algorithmic Bias and Discrimination

Technologies marketed as neutral and objective often amplify historical biases, making them harder to detect or contest.[59] Historical prejudices, once visible in the actions of individuals, can now be embedded in datasets and algorithms that present themselves as scientific.[60] This shift makes discrimination not only more pervasive but also less transparent.[61]

The consequences are concrete and well-documented globally. In the United States, the COMPAS recidivism prediction system was found to mark Black defendants as high risk at nearly twice the rate of white defendants, despite similar criminal records.[62] In the Netherlands, the SyRI welfare fraud detection system was struck down by a court for opacity and discrimination.[63] India, with its deep social stratifications of caste, religion, and gender, faces particularly acute risks from the uncritical deployment of algorithmic systems trained on historically biased data.

5.4 The Principle of Natural Justice and Algorithmic Accountability

The principle of natural justice faces unprecedented challenges from algorithmic decision-making systems. The Supreme Court's emphasis in Olga Tellis v. Bombay Municipal Corporation (1986) on both "the right to be heard from, and the right to be told why" establishes that procedural fairness encompasses the explanation of reasoning.[64] This is precisely what current AI systems cannot provide.[65] When life and liberty are at stake, the opacity of algorithms cannot be tolerated.[66]

5.5 Sectoral Algorithmic Deployments in India

Algorithmic decision-making has penetrated multiple sensitive sectors in India:

- Financial Services: The Reserve Bank of India's Guidelines on Digital Lending govern AI-powered digital lending decisions and stipulate customer protection measures and data privacy obligations on regulated entities.[67]
- Law Enforcement: Law enforcement agencies employ algorithmic tools for surveillance, pattern detection, suspect

identification, and predictive assessment of digital behaviour.[68] In 2025, the Tamil Nadu Facial Recognition Case sanctioned penalties on the harvesting of biometric data without consent, applying constitutional rights to automated surveillance.[69]

- Healthcare: The Ministry of Health and Family Welfare is developing guidelines for AI in healthcare, including telemedicine and diagnostic AI systems.[70]
- Capital Markets: The Securities and Exchange Board of India (SEBI) has issued emerging guidelines for AI use in capital markets, including algorithmic trading and robo-advisory services.[71]

VI. THE DPDP ACT AND ALGORITHMIC ACCOUNTABILITY: STRENGTHS AND GAPS

6.1 What the DPDP Act Gets Right

The DPDP Act represents a significant step forward for data protection in India. Its consent-centric framework, rights of data principals, and the establishment of the Data Protection Board create a foundation upon which algorithmic accountability can be built. The Act's extra-territorial reach ensures that foreign AI companies offering services in India are subject to its provisions.[72]

The Act's purpose limitation and data minimisation principles, requiring that Data Fiduciaries collect personal data only for specified, explicit, and legitimate purposes[73], impose constraints on the indiscriminate data harvesting that fuels many algorithmic systems. The right to erasure and correction, while limited, provides individuals with some agency over the data that feeds algorithmic profiles.

6.2 Critical Gaps in Addressing Algorithmic Decision-Making

However, the DPDP Act, 2023, though significant, barely addresses issues like algorithmic audits, bias detection, or transparency.[74] The legislation does not fully address the unique challenges posed by AI, such as algorithmic bias, lack of transparency, and issues of accountability in automated decision-making.[75] These gaps have significant implications as AI applications become more prevalent in sensitive areas like healthcare, finance, and law enforcement.[76]

Specifically, the following critical gaps can be identified:

Absence of a Right to Explanation: Unlike the GDPR, which provides data subjects with rights in relation to automated decision-making, the DPDP Act contains no explicit right to an explanation of algorithmic decisions. Current Indian laws do not mandate transparency in AI-based decision-making processes, leaving individuals with limited rights to understand or contest AI-driven decisions.[77]

No Standards for Algorithmic Accountability: Without clear standards for algorithmic accountability, it becomes challenging to hold organisations responsible for AI-driven privacy violations.[78] This gap creates a regulatory void where companies may not feel compelled to ensure AI ethics and accountability.[79]

Regulates Data, Not Algorithms: The Act regulates data, not how intelligent algorithms operate.[80] An algorithm may process data in full compliance with consent requirements and still cause disparate harm through discriminatory outputs, a challenge the DPDP Act does not directly address.[81]

Broad Government Exemptions: The wide exemptions granted to government bodies for national security and public order purposes create significant space for opaque algorithmic surveillance without judicial or legislative oversight.[82] State exemptions or blanket permissions could subvert the right to privacy, particularly in the context of mass surveillance through facial recognition and predictive policing.[83]

Absence of Sensitive Data Protections: The Act's failure to provide heightened protection for sensitive categories of personal data, such as health data, biometric data, financial data, and caste or religious identity, is particularly problematic in the algorithmic context, where such data is most frequently weaponised.[84]

VII. SIGNIFICANT DATA FIDUCIARIES AND ALGORITHMIC OVERSIGHT

7.1 The SDF Framework

The DPDP Act's most significant contribution to algorithmic governance is the framework for Significant Data Fiduciaries (SDFs). The introduction of SDFs under the DPDP Act and the operational specifics under the DPDP Rules, 2025

marks a structural shift in the way large-scale, high-impact data processors will be regulated in India.[85]
Section 10 of the DPDP Act empowers the Central Government to designate any Data Fiduciary as an SDF after considering factors including: the volume and sensitivity of personal data processed, risks to the rights of Data Principals, and potential impact on national sovereignty and security.[86] This enables the Government to classify entities based on actual risk, not merely size.[87] For example, a medium-sized genetic-testing startup could be designated an SDF because of the sensitivity of the genomic data it handles, whereas a large logistics company might not be.[88]

7.2 SDF Obligations Under Rule 13
Rule 13 of the DPDP Rules imposes several enhanced obligations on SDFs that represent the Act's most direct engagement with algorithmic accountability:
Annual DPIAs and Audits: Every SDF must undertake a Data Protection Impact Assessment and an audit once every twelve months to ensure effective observance of the provisions of the Act.[89] The DPIA reviews how personal data is processed and identifies privacy risks, while the audit checks whether the organisation is complying with the DPDP Act and its rules.[90]

Submission of Findings: The SDF must cause the person carrying out the DPIA and audit to furnish to the Data Protection Board a report containing significant observations.[91] Where a DPIA reveals algorithmic bias in content recommendations affecting user privacy, the SDF must ensure the auditor submits a report highlighting this observation along with a remediation plan.[92]

Algorithmic Due Diligence: Rule 13(3) requires that a Significant Data Fiduciary observe due diligence to verify that technical measures — including algorithmic software — adopted by it for hosting, display, uploading, modification, publishing, transmission, storage, updating, or sharing of personal data are not likely to pose a risk to the rights of Data Principals.[93] This includes ensuring algorithms do not cause unfair outcomes or misuse personal information.[94]

Appointment of Data Protection Officer: SDFs must appoint an India-based Data Protection Officer who reports directly to the Board of Directors and serves as the primary contact for grievance redressal.[95]

7.3 Limitations of the SDF Framework
While the SDF framework represents a meaningful advance, it has significant limitations. The SDF designation is discretionary; the Central Government determines which entities are designated, creating potential for regulatory capture or politically motivated exemptions. The framework also lacks quantifiable thresholds, creating uncertainty for entities seeking to assess their compliance obligations. Most critically, the algorithmic due diligence obligation under Rule 13(3) is framed in negative terms ("not likely to pose a risk") rather than imposing affirmative obligations of explainability, fairness, or non-discrimination.

VIII. COMPARATIVE ANALYSIS: INDIA, THE EU, AND THE UNITED STATES

8.1 The European Union: A Comprehensive Model
The European Union has developed the world's most comprehensive regulatory framework for both data protection and AI governance. The General Data Protection Regulation (GDPR) provides robust protections for personal data, including explicit consent requirements, the right to be forgotten, and strict rules on cross-border data transfers.[96] Crucially, Article 22 of the GDPR provides individuals with the right not to be subject to a decision based solely on automated processing that significantly affects them, and the right to obtain human intervention and an explanation of the decision.

The EU AI Act, notified in 2021, sets out a risk-based classification system for AI ranging from minimal to unacceptable and imposes strict requirements on high-risk AI applications, particularly in sensitive sectors like healthcare and law enforcement.[97] Together, these frameworks create a comprehensive regulatory environment that balances AI innovation with individual rights and privacy.[98] The EU framework adopts a risk-based approach that categorises AI systems by their potential for harm and mandates increasingly stringent requirements for higher-risk applications.[99]

8.2 Comparison with the DPDP Act
The DPDP Act and the GDPR share similar principles but differ in key aspects.[100] The DPDP Act applies only to digital personal data, while the GDPR

covers all forms of personal data.[101] More significantly, the DPDP Act's "blacklist" approach to cross-border transfers permitting data to be transferred to any country unless the Central Government specifically restricts it is simpler and more permissive than the EU's GDPR approach, which restricts transfers by default and requires adequacy determinations.[102]

The absence of a right to explanation for automated decisions, the lack of heightened protections for sensitive data, and the broad government exemptions collectively place the DPDP Act considerably behind the GDPR in terms of algorithmic accountability.

8.3 The United States: Sectoral Regulation

The United States lacks a comprehensive federal data protection law, relying instead on a patchwork of sectoral regulations. However, the Federal Trade Commission has increasingly used its unfair practices authority to challenge algorithmic discrimination, and several states have enacted AI-specific legislation. India's situation is distinct in that it has enacted a comprehensive national data protection law while lacking an AI-specific regulatory framework, the inverse of several US states.

IX. JUDICIAL TRENDS ON ALGORITHMIC GOVERNANCE IN INDIA

9.1 Constitutional Foundations for Algorithmic Challenges

Indian constitutional law offers firm ground for challenging algorithmic bias.[103] The right to privacy recognised in Puttaswamy, the guarantees of equality under Articles 14, 15, and 16, and the principles of natural justice all extend to decisions made by machines.[104] These doctrines demand transparency, reasoned explanation, and fairness — qualities not present in current AI deployments.[105]

By affirming privacy as intrinsic to life and liberty, the Puttaswamy judgment laid the groundwork for contesting opaque algorithmic systems.[106] Importantly, it framed privacy not just as protection from intrusion but also as the right to make autonomous decisions and demand explanations for state actions.[107] Justice Chandrachud's statement that privacy includes the right "to be told why" is especially relevant to algorithmic decision-making.[108]

9.2 Emerging Jurisprudence

Lower courts are beginning to address cases involving algorithmic decision-making in credit scoring, employment, and government services, though comprehensive jurisprudence is still developing.[109] In Deepak Arora (2024), the Court warned against reliance on algorithmic material to aid judicial understanding, emphasising that algorithms cannot be ascribed authorship.[110] The Supreme Court has expressed concern about the transfer of human judgment to machines.[111]

The Anuradha Bhasin v. Union of India (2020) judgment, while concerning internet shutdowns, established important principles about the proportionality of state action in the digital sphere that are directly applicable to algorithmic governance.

9.3 Automated Decision-Making and Administrative Law

There is a long history of administrative law jurisprudence in India aimed at ensuring that administrative action ascribes to constitutional principles — including rights against arbitrary state action, administrative and procedural fairness, and equality before the law.[112] Even as algorithmic systems fundamentally alter the characteristics of administrative action, there has been little consideration given to legal or regulatory responses to ensure adherence to recognised principles of administrative law.[113]

The use of algorithmic systems for administrative decision-making requires deliberating trade-offs between their presumed benefits (reducing costs, increasing efficiency, curtailing arbitrariness) and perceived harms (increasing opacity, reducing accountability).[114] These trade-offs must be deliberated within the context of specific legal frameworks, including constitutional rights that place constraints on state action.[115]

X. PERSONAL OPINION: A CRITICAL ASSESSMENT

Having examined the DPDP Act, 2023 in detail, I find myself holding a position of cautious but ultimately substantial disappointment. The Act is undeniably a historic achievement. India's first comprehensive data protection legislation, enacted after nearly a decade of deliberation, represents a

genuine legislative commitment to the constitutional right to privacy. That ought to be celebrated.

But celebration should not preclude critique.
My central concern is this: the DPDP Act was designed for a world of data processing as it existed in 2018, not for the AI-driven world of 2025 and beyond. The Act regulates how data is collected, stored, and shared. It does not regulate what happens when that data is fed into an algorithm that then makes a life-altering decision about a person. This is not a minor technical gap; it is a fundamental architectural flaw.

Consider the reality of India's digital economy today. Millions of Indians are subject to algorithmic credit scoring that determines whether they can access formal finance. Algorithmic hiring tools screen job applications before a human ever reads them. Predictive policing systems flag individuals for surveillance based on patterns in historical crime data that itself reflects decades of discriminatory law enforcement. In each of these cases, the DPDP Act provides some protection for the data that feeds the algorithm but offers no protection against the discriminatory or opaque output of the algorithm itself.

I am particularly troubled by the broad government exemptions. The Act grants the Central Government sweeping powers to exempt government entities from its provisions in the interest of national security and public order. In a country that has deployed facial recognition technology at scale without a legal framework, where predictive policing is increasingly common, and where the Aadhaar-linked data ecosystem enables surveillance at a level unimaginable in most democracies, these exemptions are not theoretical concerns; they are live threats to constitutional rights.

The absence of an independent data protection regulator is also deeply concerning. The Data Protection Board of India, whose members are appointed by the Central Government, cannot credibly be described as independent. When the largest data processor in India is the government itself, a regulator that is appointed by and accountable to the government cannot provide the structural independence necessary to protect citizens' rights. The GDPR's model of independent supervisory authorities insulated from political interference offers a better template.

At the same time, I recognise the difficult balancing act that any legislator faces in a country like India. The DPDP Act must serve the needs of a nation with 800 million internet users, a rapidly growing startup ecosystem, a complex federal structure, and profound socioeconomic inequalities. Overly prescriptive regulation could stifle innovation and impose compliance costs that disproportionately burden smaller enterprises. The Act's principles-based approach, while leaving gaps, also provides flexibility for the regulatory framework to evolve.

Ultimately, I believe India needs not just a better DPDP Act, but a dedicated AI Regulation Act that directly addresses algorithmic accountability, mandates explainability for high-stakes automated decisions, requires algorithmic impact assessments before deployment, and establishes enforceable standards of fairness and non-discrimination. The DPDP Act can and should be the foundation, but it cannot be the ceiling.

XI. RECOMMENDATIONS AND THE WAY FORWARD

Based on the foregoing analysis, the following recommendations are advanced:

11.1 Enact a Dedicated AI Regulatory Framework

India should develop an AI Regulatory Framework or Act that exists in tandem with the DPDP Act.[116] This Act should identify high-risk AI types, prescribe responsibilities of transparency and risk analysis, establish oversight bodies, determine penalties, and provide redressal mechanisms.[117] Just as environmental laws mandate environmental impact assessments, AI must require algorithmic, ethical, and human rights impact assessments.[118]

11.2 Introduce a Right to Explanation

The DPDP Act or its successor legislation should introduce an explicit right to explanation for automated decisions that significantly affect individuals. This right, modelled on Article 22 of the GDPR, should require that Data Fiduciaries provide meaningful, human-readable explanations for algorithmic decisions concerning employment, credit, healthcare, and government benefits.

11.3 Mandate Algorithmic Audits

The new rules should clearly deal with automated decision-making, fairness in algorithms, sensitive

personal data, anonymisation, liability, and cross-border transfers.[119] Preservation of audit trails, decision logs, and independent audits should be mandated.[120] Disclosure requirements on training data sources should be introduced.[121]

11.4 Establish an Independent Regulator

India should establish a standalone agency, national or semi-independent, with technical personnel, regulatory authority, investigative authority, and the power to certify high-risk systems, audit compliance, and investigate occurrences.[122] The Data Protection Board should be restructured to ensure genuine independence from the Executive.

11.5 Introduce Heightened Protections for Sensitive Data

The DPDP Act should be amended to introduce a distinct category of sensitive personal data, including health, biometric, financial, caste, religious, and sexual orientation data, with heightened protections and stricter processing requirements. This is particularly critical in the algorithmic context, where such data is most frequently used to profile and discriminate.

11.6 Regulate Government Algorithmic Deployments

The broad government exemptions in the DPDP Act must be substantially narrowed. Any government use of algorithmic systems for surveillance, predictive policing, or welfare determination should be subject to parliamentary oversight, judicial authorisation, and mandatory public disclosure.

11.7 Build Regulatory Capacity

Government agencies, regulatory bodies, and courts must develop technical expertise and capacity.[123] AI, algorithm, and data science training of regulators, judges, and law enforcers is essential for effective governance.[124]

XII. CONCLUSION

The Digital Personal Data Protection Act, 2023, represents a landmark in India's legal history, a long-overdue legislative response to the constitutional mandate of Puttaswamy and the urgent demands of a digital economy. Its consent-centric framework, rights of Data Principals, and the Significant Data Fiduciary regime provide meaningful, if incomplete, protections for individuals in the digital age.

Yet the Act's silence on algorithmic accountability, its failure to directly address the opacity, bias, and discriminatory potential of AI decision-making systems, represents a significant and increasingly urgent gap. As AI systems continue to collect, analyse, and interpret vast amounts of personal data, questions about the ethical use of AI, data protection, and individual rights are becoming central.[125] The Act was designed for a world of data processing; it must evolve to govern a world of algorithmic decision-making.

India's constitutional framework, with its robust guarantees of equality, privacy, and procedural fairness, provides the normative foundation for a more ambitious regulatory project. The right to privacy recognised in Puttaswamy, the equality guarantees of Articles 14 and 15, and the principles of natural justice articulated across decades of administrative law jurisprudence all demand that algorithmic systems be held to the same standards of transparency, reasonableness, and accountability as human decision-makers.

The question is not whether India will regulate algorithmic decision-making; the constitutional compulsion is clear. The question is whether it will do so proactively, with a comprehensive framework that protects citizens' rights while enabling responsible innovation, or reactively, after algorithmic harms have become entrenched and irreversible. The answer to that question will define the character of India's digital democracy for generations to come.

FOOTNOTES AND BIBLIOGRAPHY

Footnotes

[1] Cookie-Script, India's Digital Personal Data Protection Act (DPDPA) (2025) ("With over 800 million internet users and one of the world's fastest-growing digital economies…").

[2] Virtuosity Legal, Algorithmic Discrimination in India's Legal System: Constitutional Challenges and Policy Reform (October 13, 2025).

[3] Record of Law, Regulation of Artificial Intelligence in India: Balancing Innovation, Privacy and Accountability (March 2026).

[4] Virtuosity Legal, Algorithmic Discrimination in India's Legal System (2025).

[5] Wikipedia, Digital Personal Data Protection Act, 2023 (accessed April 2026): "On 11 August 2023, Draupadi Murmu, President of India, gave assent to the Digital Personal Data Protection Bill, 2023."

[6] Future of Privacy Forum, The Digital Personal Data Protection Act of India, Explained (2023).
[7] DLA Piper, Data Protection Laws in India (February 2026).
[8] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300; Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295. See also Supreme Court Observer, Puttaswamy v. Union of India Case Background.
[9] Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., (2017) 10 SCC 1. The Supreme Court held that the Right to Privacy is a fundamental right protected under Article 21 and Part III of the Indian Constitution.
[10] Global Freedom of Expression, Columbia University, Puttaswamy v. Union of India (I).
[11] Supreme Court Observer, K.S. Puttaswamy v. Union of India (2017).
[12] Puttaswamy (2017): M.P. Sharma and Kharak Singh were overruled.
[13] Manupatracademy, Justice KS Puttaswamy and Ors. v. Union of India (UOI), MANU_SC_1044_2017.
[14] IndConLawPhil, The Supreme Court's Right to Privacy Judgment I: Foundations (August 27, 2017).
[15] Puttaswamy (2017): The court adopted the three-pronged test of legality, necessity, and proportionality.
[16] Global Freedom of Expression, Columbia University, Puttaswamy v. Union of India (I).
[17] South Asian TransLAW Database, Justice K.S. Puttaswamy v. Union of India — Privacy.
[18] Hindu College Gazette, Privacy in India: Unpacking the Jurisprudence Behind and Impact After Puttaswamy Judgment (November 2025).
[19] Manupatracademy, Justice KS Puttaswamy, MANU_SC_1044_2017.
[20] Virtuosity Legal, Algorithmic Discrimination in India's Legal System (2025).
[21] DLA Piper, Data Protection Laws in India (2026).
[22] Manupatracademy, Justice KS Puttaswamy, MANU_SC_1044_2017.
[23] Wikipedia, Digital Personal Data Protection Act, 2023.
[24] Anantam IAS, Data Protection Act 2023: Key Provisions (2025).
[25] Wikipedia, Digital Personal Data Protection Act, 2023.
[26] Ibid.
[27] Future of Privacy Forum, The Digital Personal Data Protection Act of India, Explained (2023).
[28] Ibid.: "India, the most populous country in the world with more than 1.4 billion people, is the largest democracy and the 19th country among the G20 members to pass a comprehensive personal data protection law."
[29] Hogan Lovells, India's Digital Personal Data Protection Act 2023 Brought into Force (2025).
[30] DLA Piper, Data Protection Laws in India (February 2026): Full compliance expected by May 13, 2027.
[31] Ibid.
[32] DLA Piper, Data Protection Laws in India (2026).
[33] Ibid.
[34] Ibid.
[35] Hogan Lovells, India's Digital Personal Data Protection Act 2023 Brought into Force (2025).
[36] Ibid.
[37] Ibid.: "Notably and in contrast to other international data protection frameworks, the DPDPA treats all personal data uniformly, without imposing heightened obligations for sensitive personal data."
[38] Anantam IAS, Data Protection Act 2023: Key Provisions (2025).
[39] Ibid.
[40] PRS India, The Digital Personal Data Protection Bill, 2023.
[41] Digital Personal Data Protection Bill, 2023, Clause 6(3).
[42] Anantam IAS, Data Protection Act 2023: Key Provisions (2025).
[43] PRS India, The Digital Personal Data Protection Bill, 2023.
[44] Ibid.
[45] EY India, Decoding the Digital Personal Data Protection Act, 2023.
[46] PRS India, The Digital Personal Data Protection Bill, 2023.
[47] Future of Privacy Forum, The Digital Personal Data Protection Act of India, Explained (2023).
[48] Anantam IAS, Data Protection Act 2023: Key Provisions (2025).
[49] Ibid.
[50] EY India, Decoding the Digital Personal Data Protection Act, 2023.
[51] Hogan Lovells, India's Digital Personal Data Protection Act 2023 Brought into Force (2025).
[52] Anantam IAS, Data Protection Act 2023: Key Provisions (2025).
[53] Lexology, From Algorithms to Accountability: AI Governance in India's Data Privacy Framework (March 2025).
[54] Record of Law, Regulation of Artificial Intelligence in India (March 2026).

[55] Ibid.
[56] Ibid.
[57] Virtuosity Legal, Algorithmic Discrimination in India's Legal System (2025).
[58] Ibid.
[59] Ibid.
[60] Ibid.
[61] Ibid.
[62] Ibid.: "In the United States, the COMPAS system marked Black defendants as high risk at nearly twice the rate of white defendants, despite similar records."
[63] Ibid.: "In the Netherlands, the SyRI welfare fraud system was struck down for opacity and discrimination."
[64] Olga Tellis v. Bombay Municipal Corporation, AIR 1986 SC 180. See Virtuosity Legal, Algorithmic Discrimination in India's Legal System (2025).
[65] Virtuosity Legal, Algorithmic Discrimination in India's Legal System (2025).
[66] Ibid.
[67] Lexology, From Algorithms to Accountability: AI Governance in India's Data Privacy Framework (March 2025).
[68] ShodhSamajik, Algorithmic Policing and Due Process in Cybercrime Investigations (December 2025).
[69] Record of Law, Regulation of Artificial Intelligence in India (March 2026).
[70] LawArticle.in, AI and Privacy Law in India: Navigating the Digital Transformation Through Legal Innovation (September 2025).
[71] Ibid.
[72] DLA Piper, Data Protection Laws in India (2026).
[73] Cookie-Script, India's Digital Personal Data Protection Act (DPDPA) (2025).
[74] Virtuosity Legal, Algorithmic Discrimination in India's Legal System (2025): "The 2023 Digital Personal Data Protection Act, though significant, barely addresses issues like algorithmic audits, bias detection, or transparency."
[75] Cyberlawconsulting.com, AI and Data Privacy in India: Emerging Legal and Ethical Challenges.
[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Record of Law, Regulation of Artificial Intelligence in India (March 2026): "But the Act regulates data, not how intelligent algorithms operate."
[81] Ibid.
[82] Anantam IAS, Data Protection Act 2023: Key Provisions (2025).
[83] Law Jurist, Regulating Artificial Intelligence in India: Legal Challenges, Developments, And the Way Forward (September 2025).
[84] Anantam IAS, Data Protection Act 2023: Key Provisions (2025).
[85] Mondaq, Significant Data Fiduciaries Under The DPDP Act And DPDP Rules (November 2025).
[86] Ibid.
[87] Ibid.
[88] Ibid.
[89] DPDPA.com, Rule 13: Additional Obligations of Significant Data Fiduciary.
[90] Tsaaro, Obligations of Significant Data Fiduciaries Under the DPDP Act, 2023 and DPDP Rules, 2025 (November 2025).
[91] DPDPA.com, Rule 13: Additional Obligations of Significant Data Fiduciary.
[92] Ibid.
[93] Ibid.: Rule 13(3).
[94] Tsaaro, Obligations of Significant Data Fiduciaries (2025).
[95] Legal500, The Digital Personal Data Protection Act, 2023: Comprehensive Framework (January 2026).
[96] Lexology, From Algorithms to Accountability (March 2025).
[97] Ibid.
[98] Ibid.
[99] Virtuosity Legal, Algorithmic Discrimination in India's Legal System (2025).
[100] Wikipedia, Digital Personal Data Protection Act, 2023.
[101] Ibid.
[102] Anantam IAS, Data Protection Act 2023: Key Provisions (2025).
[103] Virtuosity Legal, Algorithmic Discrimination in India's Legal System (2025).
[104] Ibid.
[105] Ibid.
[106] Ibid.
[107] Ibid.
[108] Ibid.
[109] LawArticle.in, AI and Privacy Law in India (September 2025).
[110] Record of Law, Regulation of Artificial Intelligence in India (March 2026).
[111] Ibid.
[112] CLPR Publications, Automated Administration: Administrative Law and Algorithmic Decision-Making in India.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1717032

[113] Ibid.
[114] Ibid.
[115] Ibid.
[116] Law Jurist, Regulating Artificial Intelligence in India (September 2025).
[117] Ibid.
[118] Ibid.
[119] Ibid.
[120] Ibid.
[121] Ibid.
[122] Ibid.
[123] Ibid.
[124] Ibid.
[125] Cyberlawconsulting.com, AI and Data Privacy in India: Emerging Legal and Ethical Challenges