



Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Algorithmic Sovereignty as a Constitutional Imperative: India's Digital Governance Challenge

Dr. Inderjit Kumar^a Mehak Ahuja^b

^aAssociate Professor of Law, CT Institute of Law, Jalandhar, Punjab, India ^bHead HR & Legal, Vienna Advantage (India) Pvt Ltd, India

Received 01 June 2026; Accepted 01 July 2026; Published 04 July 2026

India's accelerating digital transformation has embedded algorithms deep within governance from Aadhaar to CoWIN, DigiLocker, and the 2025 Online Gaming Act, redefining how rights, welfare, and accountability operate. Yet, as automated decision-making systems determine entitlements, surveillance, and access, they often function beyond judicial or legislative scrutiny. Drawing upon constitutional doctrines of fairness, proportionality, and reason-giving under Maneka Gandhi and Puttaswamy, this paper conceptualises algorithmic sovereignty as a constitutional imperative: the State's duty to subject algorithmic power to the discipline of constitutional accountability. Through analysis of the IT Act, DPDP Act, new criminal codes, and sectoral statutes, it demonstrates how India's digital state delegates sovereignty to code without adequate transparency, oversight, or remedy. The paper proposes a framework of algorithmic impact assessments, independent audits, and rights to explanation and human review, re-anchoring digital governance in Articles 14, 19, and 21, and restoring the rule of law over automated power.

Keywords: *algorithmic sovereignty, digital governance, constitutionalism, rule of law, artificial intelligence.*

INTRODUCTION

India is experiencing an unprecedented digital transformation, reshaping how over 1.4 billion citizens interact with the state, access welfare, and participate in public life. Algorithm-driven systems ranging from biometric identification (Aadhaar) to digital platforms for healthcare (CoWIN), education (DIKSHA), document storage (DigiLocker), and taxation (AIS) have become central to governance. Integrated platforms like the UMANG app, which consolidates over a thousand services, illustrate the growing centralisation of public administration through algorithmic technologies.

This transformation raises critical constitutional questions: who governs the algorithms that now govern citizens? Automated decision-making increasingly mediates access to welfare, audits, and public services, yet remains opaque and largely beyond oversight. Vulnerable groups, including persons with disabilities, women, non-Hindi speakers, and rural residents, face systemic barriers in accessing these digital systems. Cases of exclusion, such as ration denial due to fingerprint mismatches or wrongful delisting from welfare rolls, reveal how technological discretion can translate into de facto constitutional deprivation. Civil society investigations in Jharkhand and Telangana confirm links between data-integration failures and denial of entitlements, while grievance mechanisms often provide 'no explanation, no hearing, no remedy.'

Survey responses collected for this paper (September–October 2025) echo these qualitative findings, showing widespread frustration with opaque automated denials and strong demands for transparency, audit, and independent oversight. Respondents called for 'algorithms that explain themselves,' reflecting a need for accountability that extends beyond data rights to the grammar of constitutional governance.

The issue is not confined to public services: private-sector algorithmic systems, from fintech to real-money gaming, exert opaque influence over behaviour, often inflicting harm without recourse. While the Promotion and Regulation of Online Gaming Act 2025 addresses monetary harms, it ignores algorithmic inducements in non-monetary contexts. This paper argues that algorithmic sovereignty is a constitutional imperative. It evaluates India's statutory frameworks, the IT Act, DPDP Act, BNS/BSA/BNSS, and Online Gaming Act

against constitutional benchmarks established in *Maneka Gandhi* and *Puttaswamy*, proposing a concrete accountability architecture for automated systems.

CONCEPTUAL AND THEORETICAL FRAMEWORK

Algorithmic Sovereignty: Let's first understand the meanings of Algorithm as well as Sovereignty.

The Algorithm – The Machine's 'Law': In its most basic sense, an algorithm is a finite, step-by-step set of rules or instructions designed to process an input and produce an output. In other words, it is a coded recipe for decision-making. While this may seem purely technical, the modern legal relevance of algorithms arises not from arithmetic, but from automated decision-making. These are the systems that apply pre-set, and often undisclosed, logic to determine outcomes that affect real lives who receive a welfare subsidy, whose loan is approved, which post is flagged as misinformation, or how a criminal's 'risk' is assessed.

Sovereignty – The State's 'Law': Sovereignty is one of the oldest and most enduring principles of constitutional and international law. It denotes the supreme and ultimate authority of the State to govern itself and its people within its territory, free from external domination. In a constitutional democracy, this authority is exercised through public institutions under the Constitution, and it carries a corresponding duty of accountability to citizens. The legal challenge of the algorithmic age lies in this: when algorithms often designed, owned, or trained beyond national borders begin to decide matters central to governance, who is the real sovereign? When foreign companies' algorithms make welfare decisions, then the authority to shape fundamental rights is no longer exclusively public. Sovereignty, once defined by control over territory, must now extend to control over the logic that governs people's digital lives.

The Integrated Concept – Algorithmic Sovereignty: Algorithmic Sovereignty thus unites these two ideas. It is the assertion of a constitutional and democratic State's supreme authority over the data, models, code, and infrastructures that shape public life. More concretely, it is the power and duty to regulate, audit, and, where necessary, veto computational logic that materially affects citizens' rights, governance, or national security.

In practice, algorithmic sovereignty embodies three interlinked entitlements:

Transparency: The right of individuals and institutions to know the basis of automated decisions in terms they can act upon;

Contestability: The right to challenge those outcomes through timely human review; and

Remedy: The right to effective correction or redress when algorithmic systems cause harm.

These entitlements are not calls for universal disclosure of source code (which companies say is intellectual property), but for reasons and verifiable justification proportionate to a decision's impact, a principle long rooted in Indian administrative law's duty of reason-giving. When the State (or a private actor performing a public function) outsources decision-making to code, the constitutional duties of fairness and accountability travel with that delegation.

For example, in India's Aadhaar system, a welfare beneficiary may be denied rations if his/her biometric authentication fails, often without knowing whether the issue is technical or procedural. Algorithmic sovereignty mandates that such systems be transparent, auditable, and correctable to ensure fairness. The question, ultimately, is not merely who owns the data, but who governs the decision logic that determines access to rights and resources. Algorithmic sovereignty, therefore, is not a technical or administrative ideal; it is a constitutional imperative. It ensures that the invisible logic governing modern life remains subordinated to the Rule of Law, not the rule of code.

Constitutional Accountability in Algorithmic Governance: Algorithmic governance, by design, transfers part of the State's decision-making power to computational systems. Yet, under India's constitutional architecture, no power, whether exercised by a human officer or by code, exists outside the discipline of constitutional accountability. Foundational principles like natural justice, due process, proportionality, and non-arbitrariness apply equally to algorithmic actions, even if current laws don't explicitly mention them, since these systems affect fundamental rights.

Natural Justice and the Right to Be Heard: The maxim *audi alteram partem*, the right to be heard before an adverse decision, is not confined to courtroom procedure; it is a constitutional value that informs every administrative action affecting rights or legitimate

expectations. When an automated welfare system discontinues benefits because a biometric match fails, or when an algorithmic fraud-detection tool triggers penalties without prior notice, the affected individual is denied both awareness and opportunity to contest. The opacity of algorithmic systems thus threatens due process. Constitutional accountability requires that automated systems embed procedural safeguards equivalent to a right of hearing, including clear explanations and options for human review.

Reasoned Decisions and the Duty to Give Reasons: The Supreme Court has long held that the recording of reasons by an administrative authority excludes chances of arbitrariness and ensures a degree of fairness in the process of decision-making.¹ Therefore, a decision without reasons is arbitrary, because reasons are what make power reviewable. When an administrative authority relies on an algorithm to determine outcomes, the duty to furnish reasons cannot vanish behind a veil of technical complexity. The obligation to provide intelligible and verifiable explanations is an extension of Articles 14 and 21. Thus, algorithmic systems should ensure constitutional intelligibility, demonstrating that decisions are made rationally and align with legal and constitutional standards, rather than focusing solely on mathematical transparency.

Proportionality and Non-Arbitrariness: Following the precedent set by the *Maneka Gandhi* case, any governmental limitations or restrictions on a person's rights or freedom must pass the proportionality test. This test simply requires that the government's action must:

- (1) have a valid, lawful objective;
- (2) be effective; and
- (3) restrict rights only as necessary.

Consequently, all State algorithms for profiling or welfare eligibility must adhere to this identical proportionality standard. If the system's results are too broad, biased, or illogical, the automated decision-making system is deemed unconstitutional.

Article 14 of the Constitution provides the right to equality, which bans arbitrary action, which ultimately demands that all algorithmic decisions be justified. The State must explain

¹ *S N Mukherjee v Union of India* (1990) 4 SCC 594

why a specific model, data source, or decision limit was chosen, and must demonstrate that no less restrictive alternatives were available to achieve its objective.

Justiciability and Standards of Review: A frequent argument advanced by the State is that algorithmic models, being technical and probabilistic, are beyond judicial competence. We cannot understand, or even investigate, a subject about which nothing is known.² However, this is inconsistent with Indian constitutional tradition, where Courts have reviewed complex decisions in the past related to economic, scientific, and environmental matters; algorithmic systems are no different in principle. Courts need not re-engineer models but must ensure that the decision process is lawful, relevant factors are considered, the outcome is reasoned and proportionate, and effective remedies are available for error or exclusion.

Rights Framework in Indian Constitutional Law: Algorithmic governance implicates the core of India's fundamental rights architecture. ADM must be assessed using constitutional principles found in Articles 14, 20(3), and 21 of the Constitution.

Article 21: Due Process and the Right to Life and Personal Liberty: In *Maneka Gandhi v Union of India*, the Supreme Court has held that any "procedure established by law" under Article 21 must be fair, just, and reasonable³, thereby constitutionalising substantive due process. Algorithmic systems that determine access to welfare benefits, healthcare, or mobility, therefore, fall squarely within Article 21's protection. When opaque or irrational automation excludes individuals without human oversight or remedy, it violates the fairness and proportionality standards reaffirmed in the *Puttaswamy* case.⁴

Article 14: Equality, Non-Arbitrariness, and Substantive Fairness: Article 14 prohibits not only discriminatory classifications but also arbitrariness in State action. It was held that arbitrariness is antithetical to equality.⁵ Algorithmic systems that reproduce social or statistical biases, for instance, by ranking welfare applicants, profiling citizens, or excluding linguistic minorities, are vulnerable to challenge on the same grounds.

² Frank Pasquale, *THE BLACK BOX SOCIETY: The Secret Algorithms that Control Money and Information* (Harvard University Press 2015)

³ *Maneka Gandhi v Union of India* (1978) 1 SCC 248

⁴ *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1

⁵ *E P Royappa v State of Tamil Nadu & Anr* (1974) 4 SCC 3

In *Ajay Hasia v Khalid Mujib*,⁶ the Court emphasised that every administrative decision must be founded on rational and non-discriminatory criteria. Algorithmic design choices such as training data selection or variable weighting constitute such criteria when they directly affect rights or entitlements. Furthermore, Article 14 demands reason-giving as a form of accountability.⁷ An algorithmic outcome that cannot be explained or justified in constitutional terms violates the equality guarantee, because algorithmic opacity precludes judicial or public scrutiny. Thus, algorithmic fairness is not a matter of computational ethics but of constitutional equality.

Article 20(3): Protection Against Self-Incrimination in Automated Surveillance:

Algorithmic governance also raises concerns under Article 20(3), which protects against compelled self-incrimination. In *Selvi v State of Karnataka*, the Court held that narco-analysis and brain mapping violated Article 20(3) because they extracted information involuntarily through technology.⁸ Likewise, automated inferences of guilt or intent drawn without consent or judicial oversight constitute algorithmic self-incrimination, a modern analogue of compelled testimony prohibited by Articles 20(3) and 21.

COMPARATIVE CONSTITUTIONAL BENCHMARKS

Algorithmic sovereignty cannot be understood in isolation from global constitutional and regulatory developments. Across jurisdictions, courts and legislators have grappled with the same problem that India now faces: how to ensure that ADM remains accountable to law. The following comparative reference points are particularly instructive for the European Union's data-protection and AI regimes.

European Union: Article 22 GDPR and the EU AI Act: Article 22 of the General Data Protection Regulation (GDPR)⁹ gives individuals the right not to be subject to decisions made solely by automated processing, including profiling, if such decisions have legal or significant effects. It provides three main protections: the right to human intervention, to express a viewpoint, and to contest decisions. Solely automated decisions are only allowed under specific exceptions such as legal requirements, contractual necessity, or explicit

⁶ *Ajay Hasia Etc v Khalid Mujib Sehravardi & Ors Etc* (1981) 1 SCC 722

⁷ *Siemens Engineering & Mfg Co v Union of India & Anr* AIR 1976 SC 1785

⁸ *Selvi & Ors v State of Karnataka & Anr* (2010) 7 SCC 263

⁹ General Data Protection Regulation 2016, art 22

consent. This framework effectively grants individuals a direct right to reject any adverse decision derived purely from computer-based processing, empowering them to demand human review and appeal the outcome. Read together with Recitals 71 and 75, this provision affirms a fundamental principle of algorithmic due process: individuals must remain more than data subjects; they are constitutional subjects entitled to review and remedy.

Article 9 of the European Union Artificial Intelligence Act (2024)¹⁰ establishes Risk management requirements for 'high-risk' AI systems, including those in welfare, education, employment, credit scoring, and law enforcement. These systems must undergo ex-ante conformity assessments, ensure traceability and meet transparency standards. Article 13 (1)¹¹ requires that such AI systems be transparent enough for deployers to interpret and use outputs responsibly, while Articles 14–17¹² mandate human oversight and ongoing monitoring. Together, these rules form a precautionary framework: the greater the rights impact, the stricter the justification required. For India, these European benchmarks illustrate how algorithmic sovereignty can coexist with market innovation by grounding accountability not in ownership of technology, but in enforceable procedural guarantees.

THE INFORMATION TECHNOLOGY ACT 2000: DELEGATED GOVERNANCE AND CONSTITUTIONAL LIMITS

The Information Technology Act 2000¹³ (IT Act) remains the cornerstone of India's digital governance, addressing electronic records, digital signatures, cybercrimes and data protection. Despite several amendments, it remains silent on algorithmic decision-making (ADM), allowing opaque, automated systems to influence welfare, judicial, and administrative processes without constitutional safeguards.

Origin in UNCITRAL Model Law: The IT Act, based on the UNCITRAL Model Law on Electronic Commerce (1996), was designed to facilitate e-commerce rather than protect digital rights. Sections 8 and 10A¹⁴ validate electronic records and e-governance, enabling platforms like DigiLocker and e-Courts. However, the Act endorses the results of these systems without requiring transparency in their logic, shifting public accountability to code.

¹⁰ Artificial Intelligence Act 2024, art 9

¹¹ Artificial Intelligence Act 2024, art 13

¹² Artificial Intelligence Act 2024, arts 14–17

¹³ The Information Technology Act 2000

¹⁴ The Information Technology Act 2000, ss 8 and 10A

For example, undisclosed algorithms in the e-Courts Services App may impact case scheduling and judge allocation, risking bias in judicial administration. Without transparency, neither litigants nor lawyers can effectively challenge automated outcomes, raising concerns under Article 14's¹⁵ equality guarantees.

Intermediary Liability and Content Regulation: Section 79 grants intermediaries' conditional immunity from liability for third-party content, subject to compliance with due diligence obligations under the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.¹⁶

- Rule 3(1)(b)¹⁷ requires intermediaries to remove unlawful content upon actual knowledge or governmental order.
- Rule 4¹⁸ imposes heightened obligations on significant social media intermediaries (SSMIs), including technical capability for traceability of message originators and deployment of automated moderation tools.

Failure to comply revokes safe-harbour protection, effectively transforming a neutral intermediary into a proactive censor. Yet, the Rules contain no procedural safeguards for algorithmic moderation, no duty to disclose filtering logic, no right to explanation, and no appeal mechanism.

The pending case of WhatsApp LLC v Union of India (Delhi High Court) challenges the government's Rule 4(2) mandate requiring messaging platforms to trace the 'first originator' of messages. WhatsApp contends that this obligation would break end-to-end encryption (E2EE) and violate the right to privacy under Article 21. The High Court has observed that traceability must be balanced against privacy and free-expression guarantees under Articles 19 and 21. This judgment, when delivered, will be a landmark in this ongoing debate and will likely define the constitutional limits of encryption, traceability, and algorithmic accountability in India's digital governance.

¹⁵ The Constitution of India 1950, art 14

¹⁶ IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

¹⁷ IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 3(1)(b)

¹⁸ IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 4

Blocking and Surveillance Powers: Section 69A¹⁹ empowers the Central Government to direct intermediaries to block online content for reasons of sovereignty, integrity, or public order. The provision is operationalised through the IT (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009²⁰, under which Rule 16 imposes strict confidentiality on blocking orders. This closed regime precludes transparency or meaningful challenge.

In *Shreya Singhal v Union of India*,²¹ the Supreme Court upheld Section 69A only because it was presumed to incorporate notice, hearing, and reasoned orders. In practice, however, algorithmic flagging and filtering occur without individualised notice, eroding the *audi alteram partem* guarantee that sustained the provision's constitutionality.

Similarly, Section 69 of the IT Act 2000²² and the Interception, Monitoring and Decryption Rules, 2009 confer wide executive powers to intercept communications without judicial authorisation. These provisions predate AI-based analytics and contain no safeguards against profiling or predictive surveillance.

Data Breach and Compensation: Section 43A²³ imposes liability on “body corporates” for negligent handling of sensitive personal data, enforced through the Sensitive Personal Data or Information (SPDI) Rules, 2011.²⁴ These Rules focus on security and consent but exclude inferred or derived data generated through algorithmic analytics, the very data most relevant to automated decision-making. The adjudicatory framework under Section 46 provides only monetary compensation and excludes public authorities, leaving victims of algorithmic exclusion without any effective remedy.

Delegated Legislation and Regulatory Framework: The IT Act 2000 illustrates the central paradox of India's digital governance: a skeletal parent statute that delegates core questions of rights and accountability to executive rule-making. Section 87 empowers the Central Government to issue rules on virtually every aspect of digital activity, from intermediary liability to surveillance, without prescribing any guiding principles. This open-ended

¹⁹ The Information Technology Act 2000, s 69A

²⁰ IT (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009, r 16

²¹ *Shreya Singhal v Union of India* (2015) 5 SCC 1

²² The Information Technology Act 2000, s 69

²³ The Information Technology Act 2000, s 43A

²⁴ Sensitive Personal Data or Information (SPDI) Rules 2011

delegation has transformed the IT Act from a framework law into a continuing source of quasi-legislation, exercised through subordinate instruments with direct constitutional consequences.

From the standpoint of Article 245²⁵ and the separation-of-powers doctrine, such delegation strains the limits of permissible legislative power. The Supreme Court, beginning with *in re Delhi Laws Act*²⁶ and reaffirmed in *Ajoy Kumar Banerjee v Union of India*,²⁷ has held that Parliament may delegate details of implementation but not its essential legislative function, namely, the determination of policy, rights, and liabilities. The IT Act, by authorising the executive to prescribe the substantive conditions for speech regulation, data processing, and surveillance, effectively transfers normative choices that belong to the legislature to the executive branch.

The Act lacks substantive and procedural standards, repeatedly using ‘as may be prescribed’ in key sections, which gives the executive unchecked authority. Important rules under the Act, like the Intermediary Guidelines 2021 and Blocking Rules 2009, were never reviewed by Parliament or assessed for proportionality, despite their influence over digital governance. The IT Act has fostered administrative constitutionalism by code, where algorithmic and surveillance norms evolve through executive discretion, beyond public scrutiny. The Supreme Court in *Shreya Singhal v Union of India*²⁸ and *Anuradha Bhasin v Union of India*²⁹ underscored that restrictions on rights must be transparent, reasoned, and reviewable. Yet the confidentiality clauses in the Blocking Rules, the opacity of algorithmic moderation, and the absence of impact assessments defy these mandates.

Judicial Control and Constitutional Oversight: The constitutional limits of delegated digital regulation have been shaped primarily through *Shreya Singhal v Union of India*³⁰ and *Anuradha Bhasin v Union of India*.³¹ These cases, already discussed in earlier parts,

²⁵ Constitution of India 1950, art 245

²⁶ *In re The Delhi Laws Act, 1912, The Ajmer-Merwara (Extension v The Part C States (Laws) Act, 1950* (1951) SCR 747

²⁷ *Ajoy Kumar Banerjee & Ors Etc v Union of India & Ors Etc* AIR 1984 SC 1130

²⁸ *Shreya Singhal v Union of India* (2015) 5 SCC 1

²⁹ *Anuradha Bhasin v Union of India & Ors* AIR 2020 SC 1308

³⁰ *Shreya Singhal v Union of India* (2015) 5 SCC 1

³¹ *Anuradha Bhasin v Union of India & Ors* AIR 2020 SC 1308

collectively establish that any restriction on fundamental rights in the digital sphere must satisfy three cumulative conditions: legality, reason-giving, and proportionality.

Applied to the IT Act, these precedents impose structural duties on both Parliament and the executive.

First, delegated rules framed under Section 87 must operate within a clearly defined legislative policy; otherwise, they fail the test of legality under *Maneka Gandhi v Union of India*.³²

Second, any restriction, such as blocking, traceability, or automated moderation, must be accompanied by intelligible reasons capable of judicial review, consistent with *Shreya Singhal*.

Third, as Anuradha Bhasin clarified, executive measures affecting speech or privacy must be published, periodically reviewed, and proportionate to a legitimate aim.

These principles extend seamlessly to algorithmic governance, where code that performs public functions must remain subject to the same duties of publication, justification, and review as any other form of State action.

Implications for Algorithmic decision making (ADM): Algorithmic systems authorised under the IT Act, 2000 operate as instruments of delegated power. Their constitutional legitimacy, therefore, depends not on their technical accuracy but on whether they respect the limits that the Constitution places on delegation itself. The principle that ‘what cannot be done directly cannot be done by delegation’ applies with equal force when power is exercised through code.³³

The Act allows the executive to frame rules for implementation, but not to construct new regimes of automated discretion. When a rule or technical directive enables algorithms to decide who receives a service, what information is blocked, or how speech is prioritised, it effectively transfers legislative judgment to software. Such transfers are incompatible with

³² *Maneka Gandhi v Union of India* AIR 1978 SC 597

³³ *In re The Delhi Laws Act, 1912, The Ajmer-Merwara (Extension v The Part C States (Laws) Act, 1950* (1951) SCR 747

the In Re Delhi Laws Act³⁴ and the non-arbitrariness doctrine in *E.P. Royappa v State of Tamil Nadu*.³⁵ Algorithms may execute the law; they may not define it.

Accordingly, delegated rules under the IT Act must treat algorithmic systems as extensions of administrative authority subject to the same doctrines of reason-giving, reviewability, and proportionality that the Court has required for all State action. Yet the infirmities of the IT Act expose a deeper structural flaw, a digital state governed by executive rules but unanchored in individual rights. The DPDP Act 2023, enacted as India's first rights-based data statute, was expected to correct this imbalance. The following section evaluates whether the DPDP Act advances constitutional governance of data, or merely rearticulates administrative discretion in the vocabulary of consent.

DIGITAL PERSONAL DATA PROTECTION ACT, 2023: RIGHTS WITHOUT ALGORITHMIC REMEDIES

Architecture and Purposes; Board Powers: The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first comprehensive privacy statute enacted after the Supreme Court recognised privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v Union of India*.³⁶ As enabling legislation under the privacy protections of Article 21, its primary objective is to ensure a balance between individual rights and the lawful, transparent processing of digital personal data. Yet the Act's architecture prioritises administrative convenience and consent formalism over substantive rights protection, creating a regime of data compliance without algorithmic accountability.

The statute is structurally minimalist. It defines 'personal data' as any data about an individual who is identifiable by or in relation to such data. under.³⁷ Unlike the GDPR, it does not distinguish between controllers and processors by function, nor does it recognise 'automated decision-making' as a distinct category of risk. The Act's operative sections (Ss. 4–10) set out general principles of lawfulness, purpose limitation, data minimisation, and accuracy, but omit procedural duties such as impact assessment, algorithmic audit, or

³⁴ *Ibid*

³⁵ *E P Royappa v State of Tamil Nadu & Anr* (1974) 4 SCC 3

³⁶ *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

³⁷ Digital Personal Data Protection Act 2023

explainability. In effect, the DPDP Act regulates how data are collected and stored, not how they are used to make decisions.

The institutional cornerstone of the Act is the Data Protection Board of India, constituted under Section 18 as an adjudicatory body to enforce compliance and impose penalties. It operates administratively under the Central Government, which appoints its members, sets procedures, and can remove them for 'public interest.' This structure compromises institutional independence, contrary to the separation-of-powers rationale articulated in *Madras Bar Association v Union of India*,³⁸ which held that tribunals exercising adjudicatory powers must be free from executive control. The Board's powers are further limited to monetary penalties; it cannot order deletion of data, suspend processing, or compel algorithmic disclosure.

The DPDP Act presents a paradox: while it acknowledges privacy as a 'right to informational self-determination,' its implementation relies on administrative compliance. The lack of algorithmic requirements and the Board's restricted authority shifts privacy from a constitutional right to a regulated permission, making it governance over privacy rather than governance by rights.

RIGHTS (SECTIONS 11-14) AND OMISSIONS: NO ADM RIGHT, NO RIGHT TO HUMAN REVIEW

The DPDP Act purports to create an individual rights framework under Sections 11 to 14, yet these rights remain procedural and consent-centric, not substantive guarantees of informational autonomy. The structure of these provisions reveals a model designed to facilitate compliance, not empowerment.

The Statutory Rights Framework: Section 11 confers the right to access information about personal data processing, including the categories of data processed and the purposes of such processing. Section 12 provides for correction and erasure of inaccurate or outdated data, and Section 13 grants the right to grievance redressal through the Data Fiduciary's internal mechanism, subject to appeal before the Data Protection Board. Section 14 introduces the right to nominate another individual to exercise these rights posthumously or upon

³⁸ *Madras Bar Association v Union of India* (2021) 7 SCC 369

incapacity. While these provisions appear rights-oriented, their scope is narrowly transactional. None of them requires a data fiduciary to disclose the logic, parameters, or consequences of automated processing. The right to access information under Section 11 is confined to ‘the personal data and the processing purpose,’ without any obligation to reveal how that data influences algorithmic outcomes.

Omission of Automated Decision-Making Safeguards: A critical omission in the DPDP Act is the absence of any protection against automated decision-making or profiling. There is no analogue to Article 22 of GDPR,³⁹ which grants individuals the right not to be subjected to decisions based solely on automated processing that significantly affect them, and the corollary right to obtain human intervention and explanation. This lacuna becomes acute when viewed against *Puttaswamy (Privacy)*, which held that informational privacy entails a right to control not merely data disclosure but also the use and inferences drawn from data. Information (modern digital data) is recombinant, i.e. that data output can be used as an input to generate more data output. By regulating only the ‘input’ stage of data handling (consent, correction) and not the ‘output’ stage of algorithmic decision-making, the DPDP Act fails to safeguard the substantive dimension of privacy as autonomy. The result is a consent bureaucracy where individuals can manage their information but remain unable to challenge how that information is used by automated systems to make decisions.

Consequences for Constitutional Accountability: This omission undermines both Articles 14 and 21. Algorithmic exclusion, where decisions are made without disclosure or recourse, cannot be remedied by the Act’s limited access and correction rights. Nor does the Data Protection Board possess the power to compel explanation, suspend algorithmic operations, or order human review. The Act thereby transforms privacy from a constitutional right of agency into a statutory right of notice. Its silences on ADM leave the citizen visible to the State but blind to the logic that governs them.

CONSTITUTIONAL ANALYSIS (ARTICLES 14, 19 AND 21; PUTTASWAMY SAFEGUARDS)

The DPDP Act must be read through the constitutional triad of Articles 14, 19 and 21, which together require that any restriction on privacy or expression satisfy legality, legitimate aim,

³⁹ General Data Protection Regulation 2016, art 22

necessity, and proportionality as articulated in Justice K.S. Puttaswamy (Retd.) v Union of India.⁴⁰

Legality: Under Puttaswamy, an encroachment upon privacy must rest on a clear legislative basis defining its scope and purpose.⁴¹ The DPDP Act meets this threshold only partially. While it establishes lawful grounds for data processing, it delegates critical matters such as specification of legitimate uses, consent exemptions, and cross-border transfers to executive rule-making without clear statutory limits.⁴² This indeterminate delegation undermines the principle of legality by making it unclear when and how personal data may be processed or shared.

Legitimate Aim and Necessity: The Act's stated purpose to balance privacy with 'lawful processing for innovation and service delivery' is constitutionally permissible, yet its breadth dilutes necessity. Section 7 authorises processing 'for any function of the State' or for 'legitimate uses' notified by the Government.⁴³ These categories are open-ended and not subject to judicially enforceable criteria. In *Maneka Gandhi v Union of India*,⁴⁴ the Court held that procedural fairness is integral to liberty; a regime that allows blanket governmental discretion over data processing fails the necessity limb because less-restrictive means such as independent oversight or data-minimisation were available but not mandated.

Proportionality and Procedural Fairness: The proportionality test, reaffirmed in *Modern Dental College v State of Madhya Pradesh*,⁴⁵ requires that measures impairing fundamental rights be proportionate to the aim pursued and accompanied by procedural safeguards. The DPDP Act does not create independent or judicial oversight over the Data Protection Board, nor does it require notice, hearing, or publication before data-sharing directives. These omissions breach both Articles 14 and 21.

Article 19 and Chilling Effect: Personal-data regulation also implicates Article 19(1)(a), since surveillance or opaque data processing chills informational self-expression. The Act's wide State exemptions under Section 17(2)(a), permitting processing for 'sovereignty and public

⁴⁰ *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

⁴¹ *Ibid*

⁴² Digital Personal Data Protection Act 2023

⁴³ Digital Personal Data Protection Act 2023, s 7

⁴⁴ *Maneka Gandhi v Union of India* (1978) 1 SCC 248

⁴⁵ *Modern Dental College & Res Cen & Ors v State of Madhya Pradesh & Ors* (2016) 7 SCC 353

order’, lack proportional limits and judicial authorisation. Such unbounded discretion risks indirect censorship through data profiling, inconsistent with *Shreya Singhal v Union of India*,⁴⁶ which demanded narrow tailoring of digital restrictions.

ALGORITHMIC CRIMINAL JUSTICE UNDER THE NEW CODES (BNS/BSA/BNSS)

Statutory Context: India’s criminal justice system entered a new statutory phase on 1 July 2024, when the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA), and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) came into force, replacing the Indian Penal Code, the Indian Evidence Act, and the Code of Criminal Procedure, respectively. These codes mark a structural re-codification rather than substantive transformation; yet their intersection with digital and algorithmic evidence introduces new constitutional challenges concerning fairness, due process, and accountability.

Integration of Digital and Electronic Evidence: The BSA recognises electronic and digital records as primary evidence under Sections 61–63, maintaining continuity with Section 65B of the former Evidence Act². The scope, however, has broadened: ‘digital records’ now covers data handled by electronic devices, servers, or cloud systems, allowing algorithm-generated evidence like facial recognition and AI forensics if authenticity is proven. Yet the statute contains no requirement to disclose the technical logic, training data, or error rates of such algorithmic tools.

Procedural Implications Under the BNSS: The BNSS preserves most procedural architecture of the former CrPC while introducing provisions for electronic communication, videoconferencing, and digital warrants (Sections 530–533). It encourages electronic record-keeping and real-time investigation tools but omits procedural safeguards governing the automated generation or interpretation of digital evidence. The Code authorises the use of ‘any technology’ approved by the State for investigation or trial, a phrase broad enough to encompass algorithmic or AI-assisted methods, yet without prescribing standards of reliability or judicial scrutiny.

⁴⁶ *Shreya Singhal v Union of India* (2015) 5 SCC 1

Continuity and Constitutional Risk: The BNS, 2023, though substantially modelled on the IPC, introduces a new digital dimension to criminal law. Sections 109, 110, and 113 criminalise organised crime, petty organised crime, and terrorist acts, each explicitly encompassing offences committed through electronic or digital means. These provisions expand the scope of criminal liability into cyber-enabled conduct but remain silent on evidentiary safeguards for algorithmically generated proof. When investigative agencies rely on automated facial recognition, metadata correlation, or predictive-risk tools, the absence of statutory standards for disclosure, verification, or defence access risks transforming algorithmic outputs into unreviewable evidence, contrary to Articles 14 and 21.

Section 197 allows the state to regulate digital speech and misinformation, using broad language that enables algorithmic monitoring and opaque content moderation. This can suppress protected expression under Article 19(1)(a). As a result, increased investigative automation and extensive speech control contribute to a technically advanced yet legally vulnerable justice system. The 2023 criminal-law codes update investigation, prosecution, and speech regulation methods, but lack due-process safeguards like disclosure, contestability, and independent validation for algorithmic accountability. This enables technology to increase executive discretion more rapidly than constitutional controls can keep up.

Algorithmic Evidence and the Right to a Fair Trial: The BSA, 2023 allows digital and algorithm-generated evidence if authenticity is certified, but does not require procedural safeguards or disclosure of the underlying algorithms, data, or models used to produce such evidence. In consequence, algorithmic determinations risk acquiring evidentiary authority without transparency, a result incompatible with the constitutional guarantee of due process under Articles 14 and 21.⁴⁷

From a constitutional perspective, algorithmic evidence must satisfy the same tests of fairness, reliability, and contestability that govern human testimony. As affirmed in *Maneka Gandhi v Union of India*⁴⁸ and *Pooja Pal v Union of India*,⁴⁹ procedural fairness is inseparable from the right to know and challenge the basis of an adverse finding. This extends to digital

⁴⁷ *Maneka Gandhi v Union of India* (1978) 1 SCC 248

⁴⁸ *Ibid*

⁴⁹ *Pooja Pal v Union of India & Ors* (2016) 3 SCC 135

determinations: where a conviction or charge relies on facial-recognition matches, predictive analytics, or automated classification, the defence must be entitled to examine the model's design, training data, and error margins. Without such disclosure, the *audi alteram partem* principle becomes a formality rather than a safeguard. The BSA thus exemplifies a broader constitutional gap: rapid technological advancement has outpaced accountability. In a justice system reliant on data-driven inference, algorithms need more than technical approval; fair trial rights require clear explanations so courts and defendants can assess machine reasoning before it influences verdicts.

Predictive Tools and Risk Assessment: Loomis Cautions: The use of predictive analytics in policing, bail, and sentencing raises constitutional concerns, as these systems rely on statistical inference rather than individual assessment. While promising efficiency, such models risk undermining the presumption of innocence by treating probabilities as evidence. Indian criminal procedure, founded on Articles 20 and 21's guarantees of liberty and fairness, cannot accept automated correlation as a substitute for proof or due process.

The constitutional risks were vividly illustrated in *State v Loomis* (Wisconsin Supreme Court, 2016),⁵⁰ where the court upheld the use of the COMPAS algorithm in sentencing. However, the court established a procedural safeguard: judges must issue a warning that the COMPAS score is only a risk assessment tool and cannot be used as the sole or controlling basis for the sentence. The *Loomis* case is a landmark moment in the legal debate over algorithmic transparency and fairness because it was the first time a state supreme court addressed the conflict between a defendant's right to due process and the use of proprietary, black-box AI tools in the criminal justice system.

Applied to India, it underscores that predictive tools may assist investigation but cannot supplant judicial discretion or adversarial testing. Without transparency of inputs, weightings, and error rates, such systems violate Article 14's non-arbitrariness and Article 21's requirement of just, fair, and reasonable procedure. The BNSS, 2023 authorises extensive use of digital surveillance and predictive policing yet omits procedural safeguards for transparency, audit, or contestation. When algorithmic forecasts influence arrest, bail, or sentencing without disclosure or defence access, they displace adjudication with

⁵⁰ *State v Loomis* [2016] 881 N W 2d 749 (Wis)

probabilistic suspicion. Constitutional fidelity, therefore, demands that predictive tools remain advisory, auditable, and subject to human reasoning and judicial scrutiny lest efficiency replace justice and automation eclipse due process.

THE PROMOTION AND REGULATION OF ONLINE GAMING ACT, 2025 AND ALGORITHMIC FAIRNESS

Under the amended IT (Intermediary Guidelines) Rules, 2021, Rule 4A, notified in 2023, was introduced to regulate online real-money gaming via a Self-Regulatory Body (SRB) model. The rule empowers the government to designate one or more SRBs that verify whether a real-money game qualifies as permissible. The SRB must ensure the game does not involve wagering, adheres to due diligence obligations under Rules 3 & 4, is not accessible to minors, and includes safeguards against addiction and financial harm.

Considering the deleterious and negative impact of online money games on the individuals, families, society and the nation as outlined in the foregoing paragraphs and given the technical aspects including the very nature of the electronic medium used for online money games, the algorithms applied and the national and transnational networks involved, it is prudent and practical in the interest of general public to completely prohibit the activity of online money gaming, rather than regulation attempts.⁵¹ Thus, in August 2025, the Promotion and Regulation of Online Gaming Act, 2025 was passed. This statute is a commendable step from the government of India and marks a significant shift from regulation via intermediary rules to primary legislation. It prohibits online money games (i.e., gaming involving monetary stakes) and activities facilitating them.

However, this Act is too new for empirical assessment. There is an urgent need for research to evaluate:

- (i) whether engagement-optimising algorithms in non-monetary e-sports titles, fintech apps, and social media continue to shape behaviour through opaque profiling;
- (ii) displacement effects to offshore/grey markets (via VPNs, crypto, and alternative payments);

⁵¹ Promotion and Regulation of Online Gaming Act 2025

- (iii) enforcement capacity and coordination with intermediaries; and
- (iv) the Act's silence on algorithmic transparency, independent audits, and harm-reduction duties.

At present, we lack longitudinal evidence on post-Act patterns of compulsive use, financial stress, and youth agency. Additionally, the Act disregards judicial precedent by banning all online money game apps, regardless of skill. This contradicts Supreme Court rulings that protected 'games of skill' as a legitimate business, raising constitutional questions under the right to trade and occupation. As a result, the Act's legality is expected to be challenged in court; this has raised many questions that can be answered only in the coming times.

INDIA'S FRAGMENTED DIGITAL GOVERNANCE FRAMEWORK

The Aadhaar Act 2016: The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereafter Aadhaar Act) constitutes India's first framework for biometric identity and automated authentication. Designed to improve subsidy distribution and prevent fraud, it supports a large system of algorithmic decision-making in welfare, finance, and citizenship. Although intended for administrative efficiency, its reliance on data-driven processes raises constitutional concerns about transparency and due process in identity verification.

Statutory Scheme and Operational Architecture: The Aadhaar Act establishes the Unique Identification Authority of India (UIDAI) as the statutory body responsible for issuing twelve-digit identity numbers based on demographic and biometric data. Sections 3–6 govern enrolment; Section 7 authorises mandatory authentication for access to state-funded subsidies and services. Authentication relies on algorithmic comparison within the Central Identities Data Repository (CIDR).

Though presented as verification, this process functions as an automated determination, and an algorithmic match score decides whether an individual is genuine or 'false.' Such outcomes directly affect entitlements like rations, pensions, or employment benefits, yet the statute provides no right to explanation, review, or human intervention. Section 8(3)(c) mandates disclosure of the 'nature of information' used but not the logic of the decision itself.

Constitutional Challenges and the Puttaswamy (Aadhaar) Judgment: In Justice K.S. Puttaswamy (Retd.) v Union of India,⁵² a five-judge Bench upheld the Aadhaar Act's core provisions while striking down or reading down others. The majority accepted that Aadhaar pursued a legitimate state aim of efficient welfare delivery, but subjected it to the four-part proportionality test earlier articulated in Puttaswamy.

The Court held that Section 7 satisfied legality and necessity, but it warned that authentication systems must not lead to exclusion or denial of entitlements. Importantly, the majority recognised that biometric verification operates on probabilistic logic, not certainty, and therefore cannot be treated as infallible evidence of identity. Nevertheless, the Court refrained from mandating independent audits or statutory remedies for wrongful exclusion, deferring instead to executive assurances.

Justice Chandrachud's dissent remains the most comprehensive constitutional critique. He characterised Aadhaar as a surveillance architecture incompatible with informational self-determination, observing that the Act enables 'pervasive profiling' and violates the principle of limited government. The dissent affirmed that the right to privacy includes control over the disclosure and use of personal data, a safeguard that the Aadhaar framework fails by compelling continuous authentication without consent or remedy.

Algorithmic Exclusion and Administrative Accountability: Several news reports since 2016 confirm that Aadhaar's automated authentication has led to exclusion through biometric errors, poor connectivity, or database inconsistencies routinely resulting in benefit denial. Such failures implicate Articles 21 and 14. Yet the Act provides no mechanism for affected persons to obtain reasons or seek prompt rectification. Administrative review remains ad hoc, confined to UIDAI's internal grievance cell.

The absence of algorithmic explainability also undermines judicial review. When a decision depends on a match score or risk flag generated by a proprietary algorithm, courts cannot assess legality without access to technical documentation. This creates a constitutional paradox: state actions remain formally subject to review but practically insulated from scrutiny by the opacity of code.

⁵² *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1

JUDICIAL AND LEGISLATIVE IMPLICATIONS

The Aadhaar rulings leave three constitutional principles unresolved:

1. Can an algorithmic authentication system with false negatives meet Article 14's non-arbitrariness standard?
2. Does allowing automated identity checks without review violate Article 21?
3. What judicial or legislative oversight is constitutionally required to prevent abuse?

Horizontal Laws Affecting Algorithms: Horizontal statutes like the RTI Act, Competition Act, Consumer Protection Act, and RPwD Act influence algorithms across sectors and promote transparency, fairness, and equality. However, these laws are technologically outdated and do not regulate algorithmic logic, explainability, or contestability, resulting in unresolved rights protection issues.

Statutes	Primary Objective	Relevance to Algorithmic Governance	Current Coverage / Action	Constitutional or Procedural Gaps
Right to Information Act 2005	Ensure transparency and access to public information (Art. 19(1)(a))	Could enable disclosure of algorithmic decision logic in public systems	Disclosure limited to outputs; source code withheld as 'IP' or 'Internal Deliberation'	No right to explanation; excludes algorithmic reasoning from transparency framework
Competition Act 2002	Prevent anti-competitive conduct and abuse of dominance	Potential to address algorithmic collusion, self-preferencing,	CCI investigations in Matrimony.com v Google (2018); 2023–24 studies	Focus on market effects, not decision logic; no audit or fairness

		and market opacity	on data-driven markets; Digital Competition Bill 2024 pending	duties for algorithms
Consumer Protection Act 2019	Safeguards consumer rights and fair-trade practices	Regulates e- commerce and AI-driven marketing	E-Commerce Rules 2020 (Rule 6) require disclosure of ranking parameters; CCPA advisories (2024) on AI ads.	Disclosures generic; no enforceable right to contest automated rankings or dynamic pricing
Rights of Persons with Disabilities Act 2016	Ensure equality and accessibility for persons with disabilities	Mandates accessible ICT and public services	Implementation focused on physical/web access; no rules on algorithmic fairness	No standards for bias auditing or inclusive data; algorithmic discrimination unaddressed

TOWARD A COHERENT FRAMEWORK FOR ALGORITHMIC SOVEREIGNTY

The empirical narratives gathered in this study converge with the constitutional analysis advanced earlier: India's digital governance, though administratively efficient, continues to operate without adequate transparency, explanation, or redress. Respondents across sectors reported algorithmic denials, opaque rejections, and limited avenues for remedy. Manifestations of a system were automation substitutes for accountability. Citizens engage daily with platforms such as Aadhaar, DigiLocker, and CoWIN, yet remain unaware of the criteria that determine access, authentication, or exclusion. These experiences expose the

jurisprudential deficit of the digital state: power exercised through code without procedural fairness. The responses consistently called for three correctives transparency in automated decisions, regulation of high-risk algorithmic systems, and institutionalised digital literacy. Read through the prism of Articles 14, 19, and 21, these demands are not policy preferences but constitutional imperatives forming the foundation of the reform proposals that follow.

RECOMMENDATIONS

Mandate Algorithmic Impact Assessments (AIAs): Every high-impact system, particularly in welfare delivery, credit scoring, policing, and taxation, should be subject to a pre-deployment AIA evaluating legality, proportionality, potential bias, and rights impact. These assessments should be made public to ensure transparency and enable independent review.

Independent Audit Bodies for Algorithmic Systems: A statutory authority or empanelled auditors should be empowered to certify, inspect, and periodically review algorithms for fairness, explainability, and compliance with Articles 14 and 21.

Regulate High-Risk Practices in Gaming, Fintech, and e-Sports Apps: Platforms using behavioural-design features and random-number generators should be required to disclose game logic, reward probabilities, and monetisation algorithms.

Expand Legal Protections in DPDP, IT Act, BNS, and Other Laws: Statutory amendments should embed explicit rights to explanation, human review, and algorithmic accountability. Such provisions would harmonise India's digital statutes with comparative safeguards found in GDPR Article 22 and the EU Artificial Intelligence Act, ensuring procedural fairness in automated decision-making.

Digital Literacy Campaigns for Algorithmic Awareness: National-level programmes, integrated into school curricula and community education, should equip citizens to understand algorithmic systems, their rights under data and privacy laws, and available mechanisms for redress. Awareness is the first defence against algorithmic exclusion.

Electoral Tech Audits to Ensure Trust and Transparency: Independent audits must be mandated for algorithmic tools used in electoral communication, political advertising, and voter analytics. Ensuring the transparency of these systems is essential to preserving public trust in democratic processes.

CONCLUSION

These reforms express the central insight of this study: that algorithmic sovereignty is constitutional sovereignty. India's challenge is not technological capacity but constitutional integration-ensuring that every algorithm exercising public power remains transparent, contestable, and humanly accountable. The rule of law must govern not only officials but also code, for in the digital republic, legitimacy depends on intelligibility.