
THE ALGORITHMIC STATE: CONSTITUTIONALISM, ARTIFICIAL INTELLIGENCE AND THE FUTURE OF DEMOCRATIC GOVERNANCE

Prabhav Mani Tiwari & Akhand Pratap Singh, BA.LLB (Hons.), Shri Ramswaroop
Memorial University, Barabanki

ABSTRACT

Artificial intelligence has moved from the periphery to the centre of public administration, reshaping the practical meaning of constitutional government. Executive agencies increasingly use automated systems to allocate welfare benefits, direct policing, verify identity, moderate public discourse and assist judicial reasoning, while legislatures and courts search for a vocabulary adequate to this shift in the character of public power. This article argues that the “algorithmic State” does not mark the end of constitutional constraint but its transformation into a new, unsettled register. It traces the constitutional principles most tested by algorithmic governance separation of powers, the rule of law, due process, equality and privacy across automated welfare administration, predictive policing, facial recognition and artificial intelligence within judicial processes. Drawing on the European Union’s Artificial Intelligence Act, the Council of Europe’s Framework Convention on Artificial Intelligence, and India’s Digital Personal Data Protection Act, 2023, IndiaAI Mission and AI Governance Guidelines, 2025, it situates Indian jurisprudence from privacy as a fundamental right to the judiciary’s recent encounters with AI-generated error within a global constitutional conversation, concluding that the future of democratic governance depends on embedding legality, transparency, accountability and human dignity into the design and oversight of algorithmic administration.

Keywords: Artificial Intelligence; Constitutionalism; Algorithmic Governance; Digital Rights; Rule of Law; Due Process; Data Protection; Judicial Review; Digital Constitutionalism; Democratic Accountability.

I. INTRODUCTION

Every generation of constitutional thought has been shaped by a distinctive anxiety about the location of power. The framers of written constitutions in the eighteenth, twentieth and midtwentieth centuries were principally concerned with the power of monarchs, legislatures, executives and standing armies; constitutionalism developed as a body of principles, structures and rights designed to ensure that such power remained accountable to law and to the people from whom it derived. The twenty-first century has introduced a form of public power that fits uneasily within this inherited vocabulary: power that is exercised not directly by an identifiable official but through automated systems capable of sorting, scoring, predicting and, with increasing frequency, deciding.

Artificial intelligence is no longer a peripheral tool of public administration. Tax authorities use machine-learning models to identify suspected instances of benefit fraud; police forces deploy facial recognition technology to identify persons of interest in public spaces; welfare and immigration agencies use automated risk-scoring to triage applications; and courts in several jurisdictions have experimented, not without controversy, with software that assists bail, sentencing and case-management decisions. Each such application promises efficiency, consistency and the removal of certain forms of human bias. Each also raises a constitutional question that existing doctrine was not designed to answer: what does it mean for a State to act lawfully, fairly and accountably when a material part of its decision-making capacity has been delegated to a system that even its own operators may not fully understand?

This article uses the term “algorithmic State” to describe a mode of governance in which algorithmic systems—machine-learning models, automated decision systems, predictive analytics and generative artificial intelligence—perform functions that were previously the preserve of human officials exercising discretion within a framework of law.¹ The phrase is descriptive rather than pejorative: it does not assume that algorithmic governance is inherently illegitimate, only that its emergence requires a form of constitutional analysis that has, until recently, been undertaken unevenly and belatedly.

1.1 The Rise of the Algorithmic State

The migration of public functions into algorithmic form has occurred gradually and, in many jurisdictions, without dedicated legislative authorisation. In the Netherlands, a self-learning

algorithm used by the tax administration to detect childcare-benefit fraud wrongly flagged tens of thousands of families disproportionately those of dual nationality for aggressive recovery action, ultimately contributing to the resignation of the Dutch government in January 2021.² In Australia, an automated debt-assessment scheme known as “Robodebt” unlawfully raised several hundred thousand welfare debts through a statistically unsound method of income-averaging that a subsequent Royal Commission found had been pursued despite internal legal warnings of its illegality, resulting in settlements that have since exceeded two billion Australian dollars.³ In the United Kingdom, the Court of Appeal held that a police force’s use of live automated facial recognition technology was unlawful for want of an adequate legal framework governing its deployment.⁴ These episodes did not arise from exotic or speculative technology; they arose from the ordinary, incremental automation of functions fraud detection, debt recovery, public-safety surveillance that States have long performed, and that written constitutions have long sought to constrain.

The Indian experience mirrors this global pattern. The world’s largest biometric identity system, Aadhaar, automated the verification of identity for welfare delivery on a scale without real precedent, prompting the Supreme Court of India to undertake one of the most extensive constitutional examinations of an algorithmic identity system anywhere in the world.⁵ Facial recognition technology has since been deployed by police forces in Delhi and other cities, by the National Crime Records Bureau through its proposed Automated Facial Recognition System, and by the Ministry of Civil Aviation through the DigiYatra programme, generally without dedicated statutory authorisation.⁶ Most recently, the Supreme Court of India has confronted the phenomenon of AI “hallucination” directly, taking cognisance of subordinate Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany’ (2021) 13(4) World Tax Journal 609; see also the account collected by the Museum of Failure, ‘Dutch Benefits Scandal’ (2025), and the parliamentary inquiry report Ongekend Onrecht (Unprecedented Injustice) (2020). courts relying on artificial-intelligence-generated citations to non-existent judgments.⁷ The algorithmic State, in other words, is not a distant prospect for India; it is already a feature of the constitutional landscape.

1.2 Constitutionalism Confronts Artificial Intelligence

Constitutionalism, in its modern sense, denotes the idea that the exercise of public power must be limited, accountable and directed towards the protection of individual rights and the

maintenance of the rule of law. Historically, these limitations were designed with a human decision-maker in mind: a minister, a magistrate, a police officer, an administrative tribunal. Doctrines such as natural justice, the duty to give reasons, proportionality and non-arbitrariness developed on the assumption that a decision could, in principle, be explained, justified and reviewed by reference to the reasoning of the person who made it.

Artificial intelligence disturbs this assumption in at least three ways. First, many contemporary machine-learning systems are opaque even to their own designers: the relationship between an input and an output may not be reducible to a set of humanly intelligible rules, a phenomenon frequently described as the “black box” problem.⁸ Second, algorithmic systems can operate at a scale and speed that outstrips the practical capacity of existing mechanisms of individual redress: a biased human official may affect dozens of individuals before detection, while a biased algorithm may affect millions before the error is even noticed. Third, responsibility for an algorithmic decision is frequently distributed across a chain of public and private actors – the agency that deploys a system, the vendor that builds it, the engineers who train it and the officials who act upon its output – in a manner that complicates the constitutional requirement that power be exercised by an identifiable, accountable authority.

These features do not mean that constitutionalism is powerless before artificial intelligence. They mean, rather, that constitutional principles must be re-articulated for a governance environment in which discretion is exercised, in part, through code. This article adopts the position – developed most systematically in the literature on “digital constitutionalism” – that such re-articulation is best understood not as a rupture with existing constitutional traditions but as their necessary evolution.

1.3 Objectives and Scope of the Study

This article examines the relationship between artificial intelligence, constitutionalism and democratic governance, with particular attention to the Indian constitutional and regulatory experience situated within a comparative global framework. It analyses the constitutional principles most directly implicated by algorithmic governance; surveys the principal domains in which artificial intelligence has entered the machinery of government; compares the regulatory responses of the European Union, the Council of Europe, the United States, China and India; and examines the emerging judicial response to algorithmic governance in India and abroad. It concludes with a set of recommendations directed at ensuring that India’s continuing

embrace of artificial intelligence in governance is accompanied by a commensurate strengthening of constitutional safeguards. The article does not treat artificial intelligence as an existential threat to constitutional government, nor as a neutral technology lying outside the reach of constitutional analysis; rather, it argues that the durability of democratic governance in the twenty-first century will depend on the capacity of constitutional law to govern the governors' own instruments of governance.

II. CONCEPTUALISING THE ALGORITHMIC STATE: THEORETICAL FOUNDATIONS

2.1 From Legal Code to Computer Code

The proposition that the character of regulation changes with the medium through which it is expressed is not new. Writing at the birth of the commercial internet, Lawrence Lessig observed that conduct in cyberspace is regulated substantially through the architecture of code itself the technical design of a system can constrain or enable behaviour as effectively as a statute, and often more effectively, since code admits of no exceptions and requires no enforcement.⁹ Lessig's insight, often summarised in the aphorism that "code is law", anticipated a central feature of the algorithmic State: that the practical content of a legal rule may come to be determined less by the text of a statute than by the manner in which that rule has been translated into the decision logic of a working system. A welfare eligibility criterion, for instance, means one thing in a statute and something subtly but significantly different once it has been encoded into the decision rules of a risk-scoring algorithm, since that encoding necessarily resolves ambiguities that the statutory text left open, and does so without the deliberative scrutiny that ordinarily accompanies delegated legislation.

2.2 Digital Constitutionalism as an Analytical Framework

A body of comparative scholarship has developed the concept of "digital constitutionalism" to describe the constitutional response to the challenges posed by digital technology. Edoardo Celeste has argued that digital constitutionalism is best understood not as a discrete set of legal norms but as an ideology a structured set of values and principles that seeks to project the aims of historical constitutionalism, namely the limitation of power and the protection of fundamental rights, onto the digital environment.¹⁰ Giovanni De Gregorio has traced the particular manner in which the European Union has pursued this project, describing a "rise of

digital constitutionalism” expressed through instruments such as the General Data Protection Regulation and, subsequently, the Artificial Intelligence Act.¹¹ Celeste and De Gregorio have further suggested that data protection law itself carries a constitutional message of “digital humanism”, under which human dignity and autonomy are asserted to outrank the efficiency claims of automated processing.¹²

This framework is useful for present purposes because it resists two equally unhelpful positions. The first treats artificial intelligence as a purely technical matter falling outside the domain of constitutional law, to be left to engineers, standards bodies and sector regulators. The second treats artificial intelligence as an unprecedented rupture that renders existing constitutional categories obsolete and calls for wholly new juridical concepts. Digital constitutionalism instead proposes continuity of value combined with discontinuity of form: the values of legality, accountability, equality and dignity remain constant, but the mechanisms by which they are secured impact assessments, algorithmic audits, explainability requirements, registers of automated decision systems must be adapted to a governance environment that earlier constitutional designers did not anticipate.

2.3 The Black Box Problem and Algorithmic Opacity

Pasquale’s account of the “black box society” identifies a specific pathology of algorithmic governance: the tendency of both commercial and governmental actors to shield the inner workings of decision-making systems from scrutiny, whether through claims of trade secrecy, technical complexity, or simple institutional inertia.¹³ The Wisconsin Supreme Court confronted precisely this problem in *State v. Loomis*, where a defendant challenged the use of a proprietary recidivism-risk-assessment tool, COMPAS, at his sentencing, arguing that its proprietary nature prevented him from testing the scientific validity of the score used to help determine his sentence.¹⁴ The Court upheld the use of the tool subject to significant caveats including that it could not be determinative of the sentence and that its known limitations had to be disclosed to the sentencing judge while nonetheless acknowledging that the assessment’s proprietary methodology limited the defendant’s ability to challenge its accuracy directly. The outcome illustrates how algorithmic opacity can coexist uneasily with due process norms that assume a decision can be interrogated on its merits.

Opacity in algorithmic governance is rarely absolute; it is more often a matter of degree and distribution. A system may be technically explicable to its designers but practically inscrutable

to the officials who rely upon it, to the individuals affected by it, and to the courts asked to review it. Constitutional analysis of the algorithmic State must therefore ask not only whether a system is explicable in principle but to whom, in what form, and at what stage of the decisionmaking process an explanation is made available.

2.4 Distinguishing Algorithmic Governance from Traditional Administrative Discretion

It might be objected that administrative law has always grappled with the delegation of discretion, and that algorithmic decision-making is simply a new instance of an old problem no different, in principle, from a minister delegating a decision to a subordinate official or a statute delegating rule-making power to an agency. There is force in this observation, and this article does not claim that algorithmic governance is entirely *sui generis*. Yet three features distinguish it in practice, if not always in principle, from earlier forms of delegation. First, unlike a human subordinate, a machine-learning system typically cannot articulate reasons for its own output in the discursive, revisable form that administrative law has traditionally required. Second, algorithmic systems are frequently deployed at a population-wide scale that magnifies the consequences of a systemic error far beyond what any individual human decision-maker could produce. Third, the commercial provenance of many algorithmic systems developed by private vendors and licensed to public authorities introduces a layer of private, often confidential, decision-making architecture between the citizen and the State that is largely without precedent in traditional administrative law. These distinguishing features justify treating the algorithmic State as a discrete subject of constitutional inquiry, even while drawing extensively on the inherited doctrines of administrative and constitutional law.

III. CONSTITUTIONAL PRINCIPLES UNDER STRAIN

3.1 Separation of Powers and the Delegation of Discretion to Machines

The doctrine of separation of powers rests on the premise that legislative, executive and judicial functions should be exercised by distinct institutions subject to mutual checks. Algorithmic governance complicates this premise by relocating a portion of what was once executive discretion into systems designed, in many cases, by private technology vendors operating outside any of the three traditional branches. When a welfare-eligibility algorithm effectively determines the scope of a statutory entitlement, or a risk-assessment tool effectively narrows the sentencing options a judge will consider, the locus of real decision-making authority shifts

from the institution formally vested with that power to the entity that designed, trained and maintains the underlying model. This is not necessarily unconstitutional legislatures routinely delegate technical rule-making to expert bodies but it does require that algorithmic delegation be subject to the same demands of authorisation, accountability and reviewability that have traditionally attached to delegated legislative and executive power.

3.2 Rule of Law and the Problem of Algorithmic Legality

The rule of law requires, at a minimum, that the exercise of public power rest upon identifiable legal authority, that the content of that authority be reasonably ascertainable in advance, and that its exercise be subject to independent review. Several of the episodes discussed in this article reveal a persistent gap between algorithmic deployment and legal authorisation. In *Bridges*, the Court of Appeal for England and Wales held that South Wales Police's use of live automated facial recognition technology was not "in accordance with the law" for the purposes of Article 8 of the European Convention on Human Rights, because the governing framework left too much discretion to individual officers as to who could be placed on a watchlist and where the technology could be deployed.¹⁵ In India, Delhi Police's own use of facial recognition technology has been shown, in a 2025 response to a Rajya Sabha question, to rest not on any statute but on an internal police order dating from June 2022 a fact that places a significant surveillance capability outside the ordinary channels of legislative authorisation and public scrutiny.¹⁶ The rule-of-law objection to such deployments is not that facial recognition technology is inherently unlawful, but that its use without a clear statutory basis defining its scope, safeguards and avenues of challenge fails to meet the legality threshold that constitutional and human rights law has long demanded of the State's coercive capacities.

3.3 Due Process and the Right to a Reasoned Decision

Due process, in its procedural dimension, ordinarily requires notice, an opportunity to be heard, and a reasoned decision capable of being understood and challenged. The Netherlands' System Risk Indication (SyRI) programme, an algorithm used to detect welfare fraud by crossreferencing data held by different public agencies, was held by the District Court of The Hague to violate the right to private life under Article 8 of the European Convention on Human Rights precisely because its underlying risk model was not disclosed even to the court, depriving affected citizens of any meaningful way of understanding why they had been flagged for investigation.¹⁷ The Court of Justice of the European Union has approached a related

question from the perspective of data protection law: in the SCHUFA case, it held that a credit-scoring agency itself engages in “automated individual decision-making” within the meaning of Article 22 of the General Data Protection Regulation where third parties rely heavily on its score to make lending decisions, even though the agency does not formally make the final decision itself.¹⁸ The practical effect of this ruling is to prevent the fragmentation of accountability across a chain of automated and human actors from defeating the individual’s right to meaningful information about, and to contest, a decision that significantly affects them.

3.4 Equality and Non-Discrimination: The Problem of Algorithmic Bias

Algorithmic systems trained on historical data risk reproducing, and in some cases amplifying, the patterns of discrimination embedded in that data. The Dutch childcare-benefits scandal offers the starkest illustration: a self-learning risk-scoring algorithm used by the Belastingdienst, the Netherlands’ tax authority, used dual nationality as an input variable and disproportionately flagged families of Caribbean-Dutch and other minority backgrounds as suspected fraudsters, precipitating aggressive debt-recovery action against an estimated twenty-six thousand families and eventually the resignation of the Dutch government in January 2021.¹⁹ Australia’s Robodebt scheme did not encode an explicit discriminatory criterion in the same manner, but its Royal Commission found that the scheme’s method of averaging annual income data to calculate fortnightly welfare debts was statistically unsound and disproportionately burdened the most vulnerable welfare recipients, who lacked the resources to contest automatically generated debts.²⁰ Both episodes illustrate a recurring feature of algorithmic bias: it is frequently invisible at the point of design, detectable only through aggregate analysis after the harm has already been inflicted upon thousands of individuals, and resistant to correction through the individual-complaint mechanisms on which equality law has traditionally relied.

3.5 Privacy and Data Protection as Constitutional Values

Privacy has emerged, across multiple jurisdictions, as the constitutional value most directly and consistently invoked against algorithmic governance, in part because so many algorithmic systems depend upon the aggregation and analysis of personal data at a scale that earlier privacy doctrine did not contemplate. The Supreme Court of India’s recognition of privacy as a fundamental right protected under Article 21 of the Constitution, examined further in Part VII below, has become the principal doctrinal anchor for evaluating algorithmic governance in the

Indian context, much as Article 8 of the European Convention on Human Rights has performed that function in *Bridges* and SyRI.²¹ What unites these developments is a recognition that privacy, in the algorithmic State, is not merely a personal interest in seclusion but a structural precondition for the individual autonomy and informational self-determination on which democratic citizenship depends.

IV. ARTIFICIAL INTELLIGENCE IN THE MACHINERY OF GOVERNMENT: APPLICATIONS AND RISKS

4.1 Automated Decision-Making in Welfare Administration

Welfare administration was among the earliest, and remains among the most consequential, sites of algorithmic governance, precisely because it combines population-scale decisionmaking with a claimant population that is frequently least equipped to contest an adverse automated determination. The Netherlands' childcare-benefits scandal and Australia's Robodebt scheme, discussed above and further below, both arose in this domain, as did the Dutch SyRI programme.²² Common to each episode is a pattern in which efficiency and fraudprevention objectives were pursued through automation without a commensurate investment in contestability: claimants were rarely given a meaningful opportunity to understand or challenge the basis of an adverse algorithmic determination before it was acted upon.

4.2 Predictive Policing and Algorithmic Surveillance

Predictive-policing tools use historical crime data to forecast the likelihood of future offending in particular locations or by particular individuals, directing police resources accordingly. Critics have observed that such tools risk perpetuating a feedback loop in which areas that have historically been over-policed generate more recorded crime data, which in turn directs further police attention to those areas, regardless of the true underlying distribution of criminal activity. In India, commentators have observed that the exemptions available to law-enforcement agencies under the Digital Personal Data Protection Act, 2023 leave predictive-policing and allied surveillance tools largely outside the Act's core protections, creating a structural asymmetry in which private actors face growing compliance obligations while State surveillance systems operate in a comparatively permissive and under-specified legal space.²³

4.3 Facial Recognition Technology in Public Spaces

Facial recognition technology occupies a distinctive place in the constitutional analysis of algorithmic governance because it operates, by design, on unconsented, ambient biometric data collected from members of the public who have taken no voluntary step to interact with the

State. In India, facial recognition systems have been deployed by police forces in Delhi, Chennai, Hyderabad, Mumbai and elsewhere, by the Ministry of Civil Aviation through the DigiYatra programme, and are proposed for nationwide expansion through the National Crime Records Bureau's Automated Facial Recognition System, which has been challenged by the Internet Freedom Foundation on the ground that its planned integration of CCTV, passport, prison and missing-persons databases raises serious digital-privacy concerns.²⁴ A response to a Rajya Sabha question in 2025 revealed that Delhi Police's own facial recognition programme operates under nothing more than an internal departmental order issued in June 2022, rather than any statute specifically regulating its use.²⁵ A private member's bill, the Facial Recognition Technology (Regulation of Police Powers) Bill, 2023, which would require magistrate-level authorisation before deployment, remains pending and, consistent with the general fate of private member's bills in India, unenacted.²⁶ The use of facial recognition technology to identify participants in the anti-Citizenship (Amendment) Act protests at Shaheen Bagh, notwithstanding its ostensible deployment for the more limited purpose of locating missing children, illustrates the phenomenon of "function creep" that civil liberties organisations have long warned accompanies surveillance infrastructure lacking clear statutory limits.²⁷ The comparative experience in *Bridges*, discussed in Part VII, suggests that Indian facial recognition deployments would struggle to satisfy the legality and proportionality tests that Article 21 of the Constitution, as interpreted in *Puttaswamy*, now demands.

4.4 Artificial Intelligence in Judicial and Quasi-Judicial Processes

Artificial intelligence has entered the judicial process both as an aid to case management and, more controversially, as a source of error within adjudication itself. The Supreme Court of India's own modernisation programme has deployed AI and machine-learning tools, developed in coordination with the National Informatics Centre and the Indian Institute of Technology, Madras, to translate judgments into eighteen Indian languages and to assist in identifying defects in electronic filings.²⁸ At the same time, the Court has confronted the risks of unsupervised AI use within the judicial process itself. In November 2025, its White Paper on

Artificial Intelligence and the Judiciary identified the fabrication of precedent by generative AI tools as a primary institutional risk and mandated the independent verification of any information obtained through such tools.²⁹ That warning proved prescient: in *Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd.*, decided on 2 July 2026, the Supreme Court set aside a trial court order that had relied on entirely fictitious, AI-generated case citations, restoring the underlying insolvency application for fresh adjudication and articulating guidelines for the responsible use of artificial intelligence within the legal profession.³⁰ A related episode arising from the Andhra Pradesh High Court, in *Gummadi Usha Rani v. Sure Mallikarjuna Rao*, involved a trial court's reliance on similarly fabricated case law; the Supreme Court held that such unverified reliance amounts not to a mere error of decision-making but to professional misconduct carrying disciplinary consequences.³¹ The Chief Justice of India has since sought to reassure the profession that artificial intelligence will remain confined to a supportive role and will not be permitted to displace independent judicial reasoning.³² Considered alongside the Delhi High Court's ruling in *ANI Media Pvt. Ltd. v. OpenAI OpCo LLC* India's first significant judicial engagement with the copyright implications of large-language-model training, in which the Court held, at the interim stage, that OpenAI's use of the news agency's content to train ChatGPT was prima facie protected as fair dealing under Section 52 of the Copyright Act, 1957 these decisions demonstrate that Indian courts are now engaging with artificial intelligence across the full range of their constitutional and adjudicatory functions: as a subject of rights-based review, as an internal institutional risk, and as a novel question of intellectual property law.³³

4.5 Artificial Intelligence, Disinformation and Electoral Integrity

Generative artificial intelligence has introduced a further governance challenge distinct from automated decision-making: the capacity to fabricate synthetic audio, video and imagery commonly termed “deepfakes” capable of undermining public confidence in the authenticity of political communication during elections. Concerns that such content might affect India's 2024 general election prompted the Ministry of Electronics and Information Technology to issue a succession of advisories, beginning in November and December 2023, requiring intermediaries to label content that could constitute misinformation or a deepfake.³⁴ An advisory issued on 1 March 2024 additionally required prior government permission before the deployment of “under-tested” or “unreliable” artificial intelligence models in India; following considerable criticism from industry, MeitY issued a Revised Advisory on 15 March 2024 that

withdrew the permission requirement while retaining, and in some respects extending, the labelling obligations.³⁵ The episode illustrates both the constitutional stakes of generative artificial intelligence for democratic self-government and the difficulty of regulating it through executive advisories issued under uncertain statutory authority rather than through primary legislation subjected to parliamentary scrutiny.

V. COMPARATIVE AND INTERNATIONAL FRAMEWORK

5.1 The European Union's Artificial Intelligence Act

The European Union's Artificial Intelligence Act, formally Regulation (EU) 2024/1689, represents the most comprehensive attempt by any jurisdiction to date to regulate artificial intelligence through a single, horizontally applicable statute.³⁶ The Act adopts a risk-based structure, prohibiting a limited category of practices considered incompatible with fundamental rights, imposing extensive documentation, testing and human-oversight obligations on systems classified as “high-risk” a category that includes many systems used in law enforcement, migration, employment and the administration of essential public services and imposing lighter transparency obligations on other systems. Notably, in 2026 the Council and the European Parliament finalised a “Digital Omnibus” package that deferred the compliance deadline for standalone high-risk systems under Annex III from August 2026 to December 2027, and for product-embedded high-risk systems to August 2028, while introducing a new prohibition, with its own December 2026 compliance date, on AI systems that generate nonconsensual intimate imagery.³⁷ This recalibration illustrates a recurring dynamic in algorithmic governance: the gap between the ambition of a regulatory framework and the practical difficulty of operationalising testing, certification and oversight infrastructure at the pace legislators originally intended.

5.2 The Council of Europe Framework Convention on Artificial Intelligence

The Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, opened for signature in Vilnius in September 2024, is the first legally binding international treaty specifically directed at artificial intelligence.³⁸ Negotiated with the participation of non-member observers including the United States, and signed by, among others, the European Union, the United Kingdom and Israel, the Convention requires parties to ensure that activities within the life cycle of AI systems remain consistent

with human rights, democracy and the rule of law.³⁹ Yet as of September 2026, the Convention illustrates the frequent gap between declaratory and operative constitutionalism at the international level: it requires five ratifications, including at least three from Council of Europe member States, to enter into force, and by that date only the European Union had deposited an instrument of ratification, on 15 May 2026.⁴⁰ The Convention's continuing non-entry into force, nearly two years after it was opened for signature, is itself a data point about the difficulty of translating international constitutional aspiration for artificial intelligence into binding legal obligation.

5.3 The United States: From Risk Management to Deregulation

The regulatory trajectory of the United States illustrates the volatility that can attend algorithmic governance where it is pursued primarily through executive order rather than legislation. President Biden's Executive Order 14110 of October 2023 had directed federal agencies to develop guidance on the safe, secure and trustworthy development of artificial intelligence, emphasising risk management, equity and the protection of civil rights.⁴¹ On his first day in office in January 2025, President Trump revoked that order by Executive Order 14148, and days later issued Executive Order 14179, "Removing Barriers to American Leadership in Artificial Intelligence", reorienting federal policy towards the removal of perceived regulatory obstacles to American AI dominance and directing the preparation of an AI Action Plan, published in July 2025.⁴² A further executive order in December 2025, "Ensuring a National Policy Framework for Artificial Intelligence", sought to establish what it termed a "minimally burdensome" national framework, reflecting continuing federal concern that a patchwork of state-level AI regulation could fragment the American regulatory environment.⁴³ The American experience over a period of little more than two years from a risk-oriented executive order, through its wholesale revocation, to a deregulatory action plan, and finally to an attempt at federal coordination of a fragmented State-level landscape underscores how contingent algorithmic governance can be on the ordinary politics of executive succession where it lacks a durable statutory foundation.

5.4 China's State-Centric Model of Algorithmic Governance

China has pursued a markedly different approach, characterised by early, granular and sectorspecific regulation issued through administrative measures rather than a single omnibus statute. Its Administrative Provisions on Recommendation Algorithms, effective March 2022,

its

Provisions on the Administration of Deep Synthesis, effective January 2023, and its Interim Measures for the Management of Generative Artificial Intelligence Services, effective August 2023, collectively require algorithm registration, content labelling and alignment with the government's social and political objectives, layered atop the pre-existing Cybersecurity Law, Data Security Law and Personal Information Protection Law.⁴⁴ A further Measures for the Administration of Labelling of Artificial Intelligence-Generated Content took effect in September 2025, mandating detectable metadata and watermarking across text, image, audio and video content.⁴⁵ The Chinese model demonstrates that algorithmic governance need not be structured around the liberal constitutional values of individual rights and limited government that animate the European and, historically, the American approaches; it can equally be structured around State control of information and alignment of technology with governmental objectives a reminder that "constitutionalism" in the algorithmic State remains a contested rather than a universally shared aspiration.

5.5 Soft Law: The OECD and UNESCO Instruments

Alongside these binding and quasi-binding instruments, a body of international soft law has sought to establish common normative ground. The OECD's Recommendation of the Council on Artificial Intelligence, first adopted in 2019 and amended in 2024 to align its definition of an AI system with that used in the European Union's Artificial Intelligence Act, and UNESCO's Recommendation on the Ethics of Artificial Intelligence, adopted in 2021, articulate principles of transparency, accountability, human oversight and proportionality that recur, in varying formulations, across the binding instruments discussed above.⁴⁶ Though not directly enforceable, such instruments perform an important function in the algorithmic State: they furnish a shared reference vocabulary against which national frameworks including India's, discussed in Part VI can be measured, even in the absence of a single binding global treaty.

5.6 Lessons for Comparative Constitutional Analysis

Three lessons emerge from this comparative survey. First, no jurisdiction has yet achieved a stable equilibrium between the promotion of artificial intelligence and its constitutional regulation; the European Union's recalibration of its own Artificial Intelligence Act, the

volatility of the American executive-order regime, and the continued non-entry-into-force of the Council of Europe's Framework Convention all point to a domain still very much in formation. Second, the choice of regulatory instrument—binding statute, binding treaty, softlaw recommendation, or executive advisory—carries constitutional significance independent of its substantive content, since it determines the degree of parliamentary and judicial accountability to which the resulting rules will be subject. Third, and most significantly for the analysis that follows, India's own regulatory trajectory has thus far favoured the least binding end of this spectrum, relying predominantly on executive advisories and non-statutory guidelines rather than dedicated primary legislation.

VI. INDIA'S EMERGING REGULATORY RESPONSE

6.1 Constitutional Foundations: Articles 14, 19 and 21

India's constitutional response to algorithmic governance rests principally upon Articles 14, 19 and 21 of the Constitution—the guarantees of equality, of the specified freedoms including speech and expression, and of life and personal liberty, respectively—as elaborated by the Supreme Court's privacy and proportionality jurisprudence examined in Part VII below. These provisions were not drafted with algorithmic governance in mind, yet their open-textured character has allowed the judiciary to extend them, incrementally, to data protection, biometric identification and digital access, in a manner broadly analogous to the extension of Article 8 of the European Convention on Human Rights to facial recognition and welfare algorithms in *Bridges* and *SyRI*.

6.2 The Information Technology Act, 2000 and Its Limits

The Information Technology Act, 2000, together with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 framed under it, remains the principal statutory basis on which the Government has sought to regulate online intermediaries, including in relation to artificial intelligence.⁴⁷ Yet the Act was drafted for an internet governed by static webpages and electronic mail, and has required successive rounds of subordinate rule-making and executive advisory to address generative artificial intelligence, a pattern examined further below. Its due-diligence and intermediary-liability framework was not designed to address the distinctive risks of foundation models capable of generating synthetic text, audio and video at scale, and commentators have consistently noted that its

application to generative AI proceeds by analogy and executive interpretation rather than express statutory design.

6.3 The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, enacted on 11 August 2023, establishes India's first comprehensive statutory framework for the processing of personal data, creating rights of access, correction and erasure for "Data Principals" and corresponding obligations for "Data Fiduciaries".⁴⁸ The Digital Personal Data Protection Rules, 2025, together with the formal establishment of the Data Protection Board of India, were notified on 13 November 2025, bringing the Act into operation on a phased basis: obligations concerning the Board's establishment took immediate effect, obligations concerning the registration of consent managers take effect in November 2026, and the Act's remaining substantive obligations including detailed notice and breach-reporting requirements are scheduled to take effect in May 2027.⁴⁹

For the purposes of the algorithmic State, the Act's most significant feature is arguably not what it includes but what it exempts. Unlike the European Union's General Data Protection Regulation, the DPDP Act contains no provision equivalent to Article 22 of the GDPR conferring a right against solely automated decision-making, and it grants government agencies broad exemptions from its core obligations where processing is undertaken in the interests of the sovereignty, integrity or security of the State, or for other specified public functions.⁵⁰ Commentators have observed that this combination the absence of an automated-decisionmaking right of the kind clarified by the Court of Justice of the European Union in SCHUFA, together with broad law-enforcement exemptions leaves precisely those algorithmic systems most in need of oversight, such as predictive-policing tools and facial recognition databases, largely outside the Act's protective core.

6.4 NITI Aayog and the National Strategy for Artificial Intelligence

India's principal public-policy think tank, NITI Aayog, published the National Strategy for Artificial Intelligence under the slogan "#AIforAll" in June 2018, identifying healthcare, agriculture, education, smart mobility and smart cities as priority sectors for AI-led development.⁵¹ It subsequently developed a three-part "Responsible AI" approach document: Part 1, setting out principles for responsible artificial intelligence, in February 2021; Part 2,

addressing the operationalisation of those principles, in August 2021; and Part 3, a discussion paper applying the framework specifically to facial recognition technology, in November 2022.⁵² The Part 3 paper is notable for having itself called for comprehensive legal reform of facial recognition technology and for recommending a recommendation not subsequently reflected in the DPDP Act's Section 17 exemptions that law-enforcement use of such technology should not be excluded from data protection oversight.⁵³

6.5 The IndiaAI Mission and the India AI Governance Guidelines, 2025

The Union Cabinet approved the IndiaAI Mission on 7 March 2024 with an outlay of ₹10,371.92 crore, structured around seven pillars including compute infrastructure, an indigenous foundation-model innovation centre, a datasets platform, start-up financing and a dedicated "Safe and Trusted AI" pillar.⁵⁴ The Mission's governance dimension matured considerably in 2025: following a January 2025 draft report prepared under the guidance of the Principal Scientific Adviser to the Government of India, the Ministry of Electronics and Information Technology released the India AI Governance Guidelines on 5 November 2025, organised around seven principles described as "Sutras" of trust, a people-first orientation, innovation over restraint, fairness and equity, accountability, systems that are "understandable by design", and safety, resilience and sustainability.⁵⁵ Rather than proposing a single comprehensive AI statute, the Guidelines favour a "lightweight", sector-agnostic approach that relies on existing sectoral regulators the Reserve Bank of India, the Securities and Exchange Board of India, the Telecom Regulatory Authority of India and others supplemented by new coordinating institutions: an AI Governance Group, a Technical and Policy Expert Committee, and an AI Safety Institute.⁵⁶ This architecture places India, alongside Japan, closer to the "lightweight", innovation-first end of the international regulatory spectrum described in Part V than to the European Union's comprehensive statutory model, a choice its architects have defended as appropriate to an economy that the Guidelines describe as the world's second-largest user base for large language models.⁵⁷

6.6 MeitY's Advisories on Generative AI and Deepfakes

In the absence of primary legislation specifically addressing generative artificial intelligence, the Ministry of Electronics and Information Technology has relied on a succession of advisories issued under the Information Technology Rules, 2021 in November and December 2023, and again on 1 and 15 March 2024 to address deepfakes and synthetic media, requiring

covered intermediaries to label AI-generated content and, in the case of the since-withdrawn permission requirement in the initial March 2024 advisory, to seek government approval before deploying “under-tested” models in India.⁵⁸ In October 2025, MeitY published draft amendments to the Intermediary Guidelines specifically addressing “Synthetically Generated Information”, proposing a “Know Your Content” provenance verification obligation for significant social media intermediaries.⁵⁹ The reliance on advisories rather than statute has attracted sustained criticism on rule-of-law grounds: as several commentators have observed, the legal basis and binding character of an “advisory” issued under the Intermediary Guidelines remains genuinely uncertain, leaving both the intermediaries subject to it and the citizens it purports to protect without a clear statutory text against which compliance, or its absence, can be measured.⁶⁰

6.7 The Regulatory Gap: Facial Recognition and Predictive Policing

The domains examined in Part IV – facial recognition and predictive policing in particular – expose the most significant gap in India’s regulatory architecture. Neither is the subject of dedicated primary legislation; both operate substantially on the strength of executive orders, procurement decisions and departmental circulars that fall outside the ordinary channels of legislative scrutiny. The Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 – a private member’s bill proposing magistrate-level authorisation before deployment – remains pending before Parliament, illustrating the broader pattern by which private member’s bills in India rarely progress to enactment regardless of the significance of the issue they address.⁶¹ Until this gap is closed by primary legislation, India’s constitutional guarantees against arbitrary State action will continue to depend disproportionately on ex post judicial review of the kind examined in Part VII, rather than on the ex ante legislative authorisation that the rule of law, as articulated in *Bridges*, has been held to require.

VII. JUDICIAL RESPONSES TO ALGORITHMIC GOVERNANCE

7.1 Indian Foundations: Puttaswamy and the Right to Privacy

The starting point for any account of Indian judicial engagement with algorithmic governance is the Supreme Court’s decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, in which a nine-judge Constitution Bench unanimously held that the right to privacy is intrinsic to the right to life and personal liberty guaranteed under Article 21 of the Constitution, as well as

being reflected in the freedoms guaranteed by Article 19.⁶² The Court articulated a threefold test for any State action infringing privacy: the existence of a valid law, a legitimate State aim, and proportionality between the means adopted and the object sought to be achieved. That has since supplied the principal doctrinal framework through which Indian courts and commentators have evaluated algorithmic and biometric governance. The judgment's significance for present purposes lies not merely in its recognition of privacy as a fundamental right but in its explicit acknowledgement of the necessity of protecting individuals from indiscriminate data collection and surveillance by State and non-State actors alike in a digital era. Language that anticipated, with some prescience, the algorithmic-governance challenges that would follow within a decade.

7.2 Aadhaar and the Limits of Algorithmic Identity Verification

The application of this framework to a concrete algorithmic system followed in *Justice K.S. Puttaswamy (Aadhaar-5 J.) v. Union of India*, in which a five-judge Bench, by a majority of four to one, upheld the constitutional validity of the Aadhaar biometric identification scheme while striking down Section 57 of the Aadhaar Act, 2016, which had permitted private entities to require Aadhaar authentication, and invalidating the mandatory linkage of Aadhaar with bank accounts and mobile telephone connections.⁶³ The majority's reasoning applied the *Puttaswamy* proportionality test directly to the design of an algorithmic identity-verification system, holding that the use of Aadhaar for the targeted delivery of welfare subsidies satisfied the test, while its extension into private commercial transactions did not. The judgment illustrates a distinctive contribution that Indian constitutional jurisprudence can make to the wider comparative conversation: rather than treating an algorithmic system as valid or invalid as a whole, it recognises that the same underlying technology may be constitutionally permissible in one application and impermissible in another, depending on the proportionality of the specific use to which it is put.

7.3 Anuradha Bhasin and Digital Access as a Constitutional Right

In *Anuradha Bhasin v. Union of India*, arising from the prolonged suspension of internet services in Jammu and Kashmir following the reorganisation of the State in August 2019, the Supreme Court held that freedom of speech and expression and the freedom to carry on trade or business through the medium of the internet enjoy constitutional protection under Articles 19(1)(a) and 19(1)(g), such that any restriction on internet access must satisfy the requirements

of Articles 19(2) and 19(6) and the test of proportionality, and that orders imposing such restrictions must be published and periodically reviewed.⁶⁴ The judgment did not go so far as to declare access to the internet an independent fundamental right, since no party had specifically sought that declaration, but its insistence on proportionality, transparency and periodic review supplies a framework directly applicable to the digital infrastructure from internet shutdowns to platform governance through which much of contemporary algorithmic governance is mediated.

7.4 The Judiciary Confronts Artificial Intelligence Directly

More recently, the Supreme Court of India has had to confront artificial intelligence not merely as a subject of constitutional review but as a source of error within the judicial process itself. In November 2025, the Court's White Paper on Artificial Intelligence and the Judiciary identified the fabrication of non-existent case law by generative AI tools as a primary institutional risk and mandated the independent verification of any AI-derived information relied upon in judicial proceedings.⁶⁵ That warning proved prescient: in *Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd.*, decided on 2 July 2026, the Supreme Court addressed a case in which a trial court had relied upon entirely fictitious, AI-generated precedents, setting aside the resulting order and articulating guidelines for the responsible use of artificial intelligence within the legal profession.⁶⁶ A parallel episode arising from the Andhra Pradesh High Court, in *Gummadi Usha Rani v. Sure Mallikarjuna Rao*, involved a trial court's reliance on similarly fabricated case law; the Supreme Court characterised such reliance not as an innocent error of legal research but as professional misconduct attracting disciplinary consequences. The Chief Justice of India has since publicly reaffirmed that artificial intelligence will remain confined to a supportive function within the judicial process and will not be permitted to substitute for independent judicial reasoning. Considered alongside the Delhi High Court's ruling in *ANI Media Pvt. Ltd. v. OpenAI OpCo LLC*, discussed in Part IV above, these decisions demonstrate that Indian courts are now engaging with artificial intelligence across the full range of their constitutional and adjudicatory functions: as a subject of rights-based review, as an internal institutional risk, and as a novel question of intellectual property law.

7.5 Comparative Judicial Approaches: Loomis, SyRI, Bridges and SCHUFA

The comparative jurisprudence surveyed throughout this article supplies four complementary judicial templates for engaging with algorithmic governance. The Wisconsin Supreme Court

in *State v. Loomis* permitted the use of a proprietary risk-assessment tool at sentencing subject to specified cautions, adopting a posture of qualified accommodation towards algorithmic decision-support.⁶⁷ The District Court of The Hague in the SyRI litigation adopted a more searching posture, invalidating an entire legislative scheme for want of the transparency necessary to satisfy the proportionality requirements of Article 8 of the European Convention on Human Rights.⁶⁸ The Court of Appeal for England and Wales in *Bridges* focused specifically on the antecedent question of legal authorisation, holding that a technology could not be assessed as proportionate at all until the legal framework governing its use was sufficiently precise.⁶⁹ The Court of Justice of the European Union in SCHUFA addressed the distinct problem of distributed accountability, ensuring that an individual's data-protection rights could not be defeated merely because the final adverse decision was formally made by an actor other than the one that generated the underlying algorithmic score.⁷⁰ Read together, these four approaches – accommodation subject to caution, invalidation for want of transparency, insistence on prior legal authorisation, and refusal to permit accountability to be diluted through distributed decision-making – supply a comparative doctrinal toolkit substantially richer than any single jurisdiction's case law could offer in isolation, and one from which Indian courts, still in the relatively early stages of confronting algorithmic governance directly, may usefully draw.

7.6 Lessons from Algorithmic Failure: The Netherlands and Australia

The Dutch childcare-benefits scandal and Australia's Robodebt scheme, discussed in Parts I, III and IV above, are not, strictly speaking, judicial decisions, but they belong in any account of the judicial and quasi-judicial response to algorithmic governance because both were ultimately unwound through legal process: a 2019 Federal Court ruling that the Robodebt income-averaging methodology was unlawful, followed by a statutory Royal Commission whose findings informed subsequent class-action settlements exceeding two billion Australian dollars;⁷¹ and, in the Netherlands, parliamentary and judicial scrutiny that established the discriminatory character of the childcare-benefits risk model and prompted the resignation of the Rutte government in January 2021.⁷² Both episodes illustrate that judicial review, however robust, frequently operates only after an algorithmic harm has already been inflicted at a population-wide scale – a limitation that strengthens, rather than diminishes, the case for the ex ante safeguards, including algorithmic impact assessments and independent oversight, recommended in Part IX below.

7.7 Towards an Emerging Principle: The Right to Explanation

Across the comparative material surveyed in this Part, a common doctrinal thread can be discerned: an inchoate but increasingly insistent judicial demand that a person affected by an algorithmic decision be given some meaningful account of the basis on which it was made, whether that demand is framed in the language of due process, of Article 8 of the European Convention on Human Rights, or of Article 22 of the General Data Protection Regulation. India's constitutional jurisprudence, through the *Puttaswamy* proportionality test and the transparency and review requirements articulated in *Anuradha Bhasin*, contains the doctrinal resources necessary to develop an equivalent "right to explanation" specific to algorithmic State action, even though, as Part IX argues, its explicit statutory articulation remains an unfinished task.

VIII. RECENT TRENDS AND THE FUTURE OF ALGORITHMIC CONSTITUTIONALISM

8.1 Global AI Governance Summitry and the India AI Impact Summit, 2026

The annual cycle of global AI-governance summitry from the Bletchley Park AI Safety Summit in the United Kingdom in 2023, through the Seoul AI Summit in 2024 and the Paris

AI Action Summit in 2025, to the India AI Impact Summit held in New Delhi from 16 to 21 February 2026 traces a discernible shift in international emphasis, from the containment of catastrophic risk towards the practical governance of AI's economic and social impact.⁷³ The India AI Impact Summit, the first such summit hosted in the Global South, drew delegations from more than one hundred countries, produced a Declaration endorsed by ninety-two countries and international organisations, and announced a substantial expansion of India's sovereign AI compute capacity.⁷⁴ Its significance for this article lies less in its specific outcomes than in its symbolic confirmation that questions of algorithmic governance can no longer be regarded as the preserve of the industrialised economies that hosted the three preceding summits; the constitutional and regulatory choices open to India carry, and will increasingly be seen to carry, systemic significance for the Global South more broadly.

8.2 Constitutional Design for Algorithmic Accountability

The comparative material surveyed in this article suggests several design principles capable of

being generalised across jurisdictions. Legal authorisation should precede deployment rather than follow it, as *Bridges* insists. Transparency obligations should extend to the underlying logic of a system and not merely to the fact of its use, as SyRI and SCHUFA together suggest. Oversight institutions should be structurally independent of the agencies whose algorithmic systems they are charged with reviewing, a lesson underscored by the Robodebt Royal Commission's finding that internal legal warnings about the scheme's unlawfulness were disregarded for years before external, independent scrutiny intervened.⁷⁵ None of these principles requires the wholesale invention of new constitutional concepts; each is a specific application of doctrines—legality, transparency, independent review—that Indian and comparative constitutional law already recognises.

8.3 Independent Oversight, Algorithmic Audits and Regulatory Sandboxes

Robodebt Royal Commission, *supra* note 3; see also reporting on the Royal Commission hearings regarding legal advice received and disregarded by the Department of Social Services.

India's AI Governance Guidelines of November 2025 gesture towards several of these design principles through their proposed AI Governance Group, Technical and Policy Expert Committee and AI Safety Institute, and through their emphasis on voluntary algorithmic audits and techno-legal accountability mechanisms.⁷⁶ Yet the Guidelines' explicitly "lightweight" character, and their deliberate choice to rely on existing sectoral regulators rather than a dedicated statutory authority, leaves open the question whether purely voluntary and advisory mechanisms can supply the independence and enforceability that the comparative case law examined in Part VII suggests are constitutionally necessary, particularly in domains—facial recognition and predictive policing—foremost among them where the relevant "sectoral regulator" is often the very law-enforcement agency whose conduct requires oversight.

8.4 Balancing Innovation, National Security and Fundamental Rights

None of the foregoing should be read as counselling indifference to the legitimate interests that algorithmic governance is frequently designed to serve. Predictive analytics can direct scarce policing resources towards genuine public-safety needs; automated systems can deliver welfare benefits to eligible citizens more quickly and at lower administrative cost than manual processing; and facial recognition technology has, on occasion, been used credibly to reunite missing children with their families. The constitutional task is not to prohibit these applications

but to ensure that the pursuit of efficiency, security and administrative convenience does not proceed at the expense of legality, transparency and equal treatment the very balance that Article 21 of the Constitution, as elaborated in *Puttaswamy*, already requires the Indian State to strike in every context, algorithmic or otherwise.

8.5 Towards Constitutionalism by Design

The most durable lesson of the comparative experience surveyed in this article may be that constitutional compliance cannot be reliably achieved after the fact, through litigation alone, once an algorithmic system has already been deployed at scale. If the Dutch, Australian and British experiences teach anything in common, it is that the constitutional values of legality, transparency and non-discrimination must be embedded in the design and procurement of algorithmic systems from the outset a principle this article terms “constitutionalism by design”, in deliberate echo of the “privacy by design” principle that already finds indirect statutory expression in India’s own Digital Personal Data Protection Act.⁷⁷ Achieving this will require India’s legislative and regulatory institutions to move beyond the advisory and guideline-based instruments that have characterised the response thus far, towards the primary legislation whose absence Part VI identified as the central gap in India’s present regulatory architecture.

IX. SUGGESTIONS AND RECOMMENDATIONS

9.1 Statutory Recognition of a Right to Explanation

Parliament should consider amending the Digital Personal Data Protection Act, 2023, or enacting dedicated legislation, to confer upon individuals a right to a meaningful explanation of any solely or predominantly automated decision that produces a legal or similarly significant effect upon them, modelled upon, but adapted from, Article 22 of the European Union’s General Data Protection Regulation as construed by the Court of Justice of the European Union in *SCHUFA*. Such a right should extend to decisions made with the assistance of a private vendor’s proprietary system, ensuring that commercial-confidentiality claims of the kind raised, ultimately unsuccessfully, in *Loomis* cannot be used to defeat an individual’s ability to understand and contest a decision affecting them.

9.2 Mandatory Algorithmic Impact Assessments for State Functions

Before any automated or algorithmic system is deployed in a function of government welfare

administration, policing, identity verification or judicial administration alike the responsible authority should be statutorily required to conduct and publish an algorithmic impact assessment addressing the system's legal basis, its training data, its expected error rates and their distribution across protected groups, and the mechanisms available for individual redress. The SyRI litigation and the Robodebt Royal Commission both illustrate the consequences of dispensing with such an assessment; the practice, developed in the United Kingdom after *Bridges*, of conducting Data Protection Impact Assessments before deploying facial recognition technology illustrates a workable, if imperfect, alternative.

9.3 Closing the State-Actor Exemption in the DPDP Act

The broad exemptions available to government agencies under Section 17 of the Digital Personal Data Protection Act, 2023 should be narrowed and made subject to independent oversight, particularly in relation to systems such as the National Crime Records Bureau's proposed Automated Facial Recognition System and other predictive-policing tools. NITI Aayog's own 2022 recommendation that law-enforcement use of facial recognition technology should not be excluded from data protection oversight offers a ready-made template that the DPDP Rules have not yet adopted, and that Parliament should now consider through amendment.

9.4 An Independent AI Regulatory and Oversight Authority

While the sector-agnostic, "lightweight" approach favoured by the India AI Governance Guidelines, 2025 has considerable merit in preserving room for innovation, the AI Governance Group and Technical and Policy Expert Committee it proposes should be placed on a statutory footing, with structural independence from the ministries and agencies whose own use of artificial intelligence they may be called upon to review, so that the pattern of internal warnings being disregarded identified by Australia's Robodebt Royal Commission is not replicated in the Indian context.

9.5 Strengthening Parliamentary and Judicial Oversight

Parliament's standing committees should be empowered, and adequately resourced, to conduct regular technical review of significant government AI deployments, including facial recognition and predictive-policing systems presently authorised only by executive order or

internal circular; and specialised judicial or quasi-judicial capacity potentially situated within the Data Protection Board of India should be developed to adjudicate algorithmic harm claims with the technical expertise that general courts, as the Supreme Court's own recent experience with AI-generated case law illustrates, cannot always be assumed to possess without dedicated institutional support.

9.6 Embedding Constitutional Values in Technical Design

Public procurement rules governing the acquisition of AI systems by government departments should require, as a condition of contract, that vendors demonstrate explainability, auditability and bias-testing appropriate to the risk classification of the intended use, translating the "constitutionalism by design" principle developed in Part VIII into an enforceable procurement standard rather than leaving it as an aspiration recited in non-binding guidelines.

9.7 International Cooperation and Interoperable Standards

Finally, India should continue to engage actively with the international instruments surveyed in Part V including eventual consideration of accession to the Council of Europe's Framework Convention on Artificial Intelligence, notwithstanding that instrument's own slow path to entry into force both to ensure interoperability of Indian AI-governance standards with those of India's major trading partners, and to allow India, as host of the 2026 AI Impact Summit and a jurisdiction second only to the United States in large-language-model usage, to shape rather than merely receive the emerging international consensus on algorithmic constitutionalism.

X. CONCLUSION

The algorithmic State is not a speculative prospect confined to the pages of technology-policy journals; it is, as this article has sought to demonstrate, an operating reality of contemporary Indian and comparative governance, visible in the biometric architecture of Aadhaar, the facial recognition cameras of Indian police forces, the risk-scoring algorithms that determined welfare entitlements in the Netherlands and Australia, and the fabricated precedents that have already reached the Supreme Court of India's own docket. The central argument of this article has been that the emergence of this algorithmic State does not require the abandonment of constitutional government, but rather its adaptation: the values of legality, proportionality, equality and human dignity that animate Articles 14, 19 and 21 of the Constitution of India,

and their analogues in comparative constitutional and human rights law, remain fully capable of application to algorithmic governance, provided that the institutions responsible for articulating and enforcing them legislatures, regulators and courts alike are equipped with the statutory tools, technical capacity and structural independence necessary to do so.

India's own trajectory illustrates both the promise and the incompleteness of this adaptation. The Supreme Court's privacy and Aadhaar jurisprudence supplies a doctrinal foundation as sophisticated as any comparable body of case law worldwide; the IndiaAI Mission and the India AI Governance Guidelines, 2025 demonstrate a serious institutional commitment to the governance, and not merely the promotion, of artificial intelligence; and the judiciary's recent, direct confrontation with AI-generated error within its own processes demonstrates an institutional self-awareness that many older and ostensibly more developed regulatory systems have yet to display. Yet the persistent reliance on executive advisories rather than primary legislation, the broad law-enforcement exemptions within the Digital Personal Data Protection Act, 2023, and the continuing absence of any dedicated statute governing facial recognition or predictive policing together reveal a regulatory architecture still some distance from the "constitutionalism by design" that this article has argued the algorithmic State ultimately requires.

As India assumes an increasingly prominent role in global AI governance a role symbolised by its hosting of the AI Impact Summit in February 2026 the choices it makes in closing these gaps will carry significance well beyond its own borders. The future of democratic governance, in India and elsewhere, will be shaped not by whether States adopt artificial intelligence, a question that has already been answered in the affirmative, but by whether they succeed in ensuring that the machinery of algorithmic administration remains, in substance and not merely in form, subject to the rule of law.

ENDNOTES:

- 1 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).
- 2 D Hadwick and S Lan, 'Lessons to Be Learned from the Dutch Childcare Allowance Scandal: A Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany' (2021) 13(4) *World Tax Journal* 609; see also the account collected by the Museum of Failure, 'Dutch Benefits Scandal' (2025), and the parliamentary inquiry report *Ongekend Onrecht* (Unprecedented Injustice) (2020).
- 3 Royal Commission into the Robodebt Scheme, Final Report (Commonwealth of Australia, 2023); 'Australia agrees to record \$309 million payout to victims of illegal debt recovery scheme', Reuters, September 2025.
- 4 *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.
- 5 *Justice K.S. Puttaswamy (Aadhaar-5 J.) v. Union of India*, (2019) 1 SCC 1.
- 6 Wikipedia, 'Automated Facial Recognition System (India)', noting the legal notice issued by the Internet Freedom Foundation to the National Crime Records Bureau; 'Facial Recognition In India: Privacy, Surveillance And The Missing Legal Framework', Outlook India, 2026.
- 7 *Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd. & Anr.*, Civil Appeal No. 11950 of 2025 (Supreme Court of India, 2 July 2026).
- 8 Pasquale, *supra* note 1.
- 9 Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999).
- 10 Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33(1) *International Review of Law, Computers & Technology* 76; Edoardo Celeste, 'Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges', HIIG Discussion Paper Series No. 2018-02 (2018).
- 11 Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2021) 19(1) *International Journal of Constitutional Law* 41.
- 12 Edoardo Celeste and Giovanni De Gregorio, 'Digital Humanism: The Constitutional Message of the GDPR' (SSRN, 2022).
- 13 Pasquale, *supra* note 1.
- 14 *State v. Loomis*, 2016 WI 68, 881 N.W.2d 749 (Wis. 2016).
- 15 *Bridges*, *supra* note 4.
- 16 'Explained: Delhi Police's AI surveillance network and why it's under scrutiny', The News Minute, 2026, citing a 2025 Rajya Sabha reply of the Ministry of Home Affairs to MP Saket Gokhale.
- 17 *NJCM c.s. and FNV v. The State of the Netherlands* (SyRI), District Court of The Hague, ECLI:NL:RBDHA:2020:1878 (5 February 2020).
- 18 *OQ v. Land Hessen* (SCHUFA Holding), Case C-634/21, Court of Justice of the European Union (7 December 2023).
- 19 *Toeslagenaffaire*, *supra* note 2.
- 20 *Robodebt*, *supra* note 3.
- 21 *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; AIR 2017 SC 4161.
- 22 See Parts I, III and VII above; *toeslagenaffaire*, *supra* note 2; *Robodebt*, *supra* note 3; SyRI, *supra* note 17.
- 23 'AI Policing and Surveillance in India', SPRF, 2026, discussing s. 17 of the Digital Personal Data Protection Act, 2023 and its exemptions for State agencies.
- Chennai, Hyderabad, Mumbai and elsewhere, by the Ministry of Civil Aviation through the
- 24 AFRS, *supra* note 6.
- 25 Delhi Police order, *supra* note 15.
- 26 'Facial Recognition in India: Privacy, Surveillance and the Need for Regulation', amlegals, 2026.
- 27 'Facial recognition in law enforcement is the litmus test for India's commitment to "Responsible AI for All"', Observer Research Foundation.
- 28 Press Information Bureau, Government of India, 'Use of Artificial Intelligence in Supreme Court' (2025).
- 29 Supreme Court of India, White Paper on Artificial Intelligence and the Judiciary (November 2025), discussed in 'Indian courts have an AI problem, and the Supreme Court is not amused', The Federal, 2026.
- 30 Pooja Ramesh Singh, *supra* note 7.
- 31 *Gummadi Usha Rani & Anr v. Sure Mallikarjuna Rao & Anr* (Supreme Court of India, 2026), discussed in 'India's SC warns against unsupervised AI use in rulings', Law.asia, 2026.
- 32 Statement of Chief Justice of India Surya Kant, reported in 'Supreme Court assures Judges exercising "Utmost Caution" on use of AI in judicial process', All India Radio News, 6 December 2025.
- 33 *ANI Media Pvt. Ltd. v. OpenAI OpCo LLC* (Delhi High Court, 2025–26), discussed in 'India's First AI Copyright

Ruling: The Delhi High Court In ANI v. OpenAI', Mondaq, 2026.

34 Ministry of Electronics and Information Technology, Advisory dated 1 March 2024; see 'Under-testing AI Models: MeitY's Advisory to Tackle Potential Risks', Fox Mandal, 2024.

35 Ministry of Electronics and Information Technology, Revised Advisory dated 15 March 2024; JSA, 'Revised MeitY Advisory on deployment of AI models', 2024.

36 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

37 Council of the European Union, 'Artificial Intelligence: Council gives final green light to simplify and streamline rules', press release, 29 June 2026; Council of the European Union and European Parliament, 'Artificial Intelligence: Council and Parliament agree to simplify and streamline rules', press release, 7 May 2026.

38 Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225 (Vilnius, 5 September 2024).

39 Council of Europe, 'The Framework Convention on Artificial Intelligence' (2026); European Commission, 'Commission signs Council of Europe framework Convention on Artificial Intelligence' (2024).

40 Council of Europe, 'European Union ratifies the Council of Europe Framework Convention on Artificial Intelligence', 15 May 2026; regulatorik.ai, 'Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS 225)' (accessed 8 September 2026).

41 Exec. Order No. 14110, 'Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence', 30 October 2023.

42 Exec. Order No. 14148, 20 January 2025; Exec. Order No. 14179, 'Removing Barriers to American Leadership in Artificial Intelligence', 23 January 2025; Squire Patton Boggs, 'Key Insights on President Trump's New AI Executive Order', 2025.

43 Mayer Brown, 'President Trump Issues Executive Order on "Ensuring a National Policy Framework for Artificial Intelligence"', 23 December 2025.

44 Cyberspace Administration of China, Interim Measures for the Management of Generative Artificial Intelligence Services, effective 15 August 2023; CMS, 'AI laws and regulations in China', Expert Guide, 2026.

45 Cyberspace Administration of China, Measures for the Administration of Labeling of Artificial Intelligence Generated Content, effective 1 September 2025, together with national standard GB 45438-2025.

46 OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (2019, as amended 2024); UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

47 The Information Technology Act, 2000; The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

48 The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

49 The Digital Personal Data Protection Rules, 2025; Lexology, 'The Digital Personal Data Protection Rules, 2025: A New Digital Frontier', 2025.

50 Digital Personal Data Protection Act, 2023, s. 17; see also SPRF, *supra* note 23.

51 NITI Aayog, National Strategy for Artificial Intelligence: #AIforAll (Government of India, June 2018).

52 NITI Aayog, Responsible AI for All: Approach Document for India, Part 1 – Principles for Responsible AI (February 2021); Part 2 – Operationalising Principles for Responsible AI (August 2021); Part 3 – Adopting the Framework: A Use Case Approach on Facial Recognition Technology (November 2022).

53 *amlegals*, *supra* note 24.

54 Press Information Bureau, Government of India, 'Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem', 7 March 2024.

55 Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines (5 November 2025); Saikrishna & Associates, 'Decoding the India AI Governance Guidelines', 2025.

56 *azb*, 'MeitY releases Guidelines on AI Governance – The Way Ahead and Roadmap for AI use in India', 2025; Lexology, 'AI Governance Guidelines', 2025.

57 Chambers and Partners, 'MeitY unveils India's Approach towards regulating Artificial Intelligence', 2025; *vajiramandravi*, 'India AI Governance Guidelines 2025', 2025.

58 *MeitY advisories*, *supra* note 34.

59 Ministry of Electronics and Information Technology, Draft Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, 22 October 2025; Lexology, 'AI Governance Guidelines', 2025.

60 ELP Law, 'Navigating AI Regulation in India: Unpacking the MeitY Advisory on AI in a Global Context', 2024; JSA, *cited above*.

61 *amlegals*, *supra* note 24.

62 *Puttaswamy*, *supra* note 21.

63 *Aadhaar-5 J.*, *supra* note 5; see also the summary in Supreme Court Observer, 'Constitutionality of Aadhaar Act: Judgment Summary'.

64 *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

65 White Paper, *supra* note 28.

66 Pooja Ramesh Singh, *supra* note 7.

67 *Loomis*, *supra* note 13.

68 SyRI, *supra* note 17.

69 *Bridges*, *supra* note 4.

70 SCHUFA, *supra* note 18.

71 Robodebt, *supra* note 3.

72 Toeslagenaffaire, *supra* note 2.

73 Wikipedia, 'India AI Impact Summit 2026'; Center for Strategic and International Studies, 'India's AI Impact Summit'.

74 Press Information Bureau, Government of India, 'India AI Impact Summit 2026: Landmark Global Declaration and Major AI Investment Commitments', 2026.

75 Robodebt Royal Commission, *supra* note 3; see also reporting on the Royal Commission hearings regarding legal advice received and disregarded by the Department of Social Services.

76 AI Governance Guidelines, *supra* note 55.

77 Digital Personal Data Protection Act, 2023, *supra* note 48.

BIBLIOGRAPHY

A. Constitutional and Statutory Materials (India)

1. The Constitution of India, 1950.
2. The Information Technology Act, 2000.
3. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
4. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
5. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
6. The Digital Personal Data Protection Rules, 2025.
7. The Copyright Act, 1957.

B. International and Comparative Instruments

8. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
9. Regulation (EU) 2016/679 (General Data Protection Regulation).
10. Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225 (Vilnius, 5 September 2024).
11. European Convention on Human Rights, 1950.
12. OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (2019, as amended 2024).
13. UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).
14. Cyberspace Administration of China, Interim Measures for the Management of Generative Artificial Intelligence Services (effective 15 August 2023).
15. Cyberspace Administration of China, Measures for the Administration of Labeling of Artificial Intelligence-Generated Content (effective 1 September 2025).
16. Exec. Order No. 14110, 'Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence' (30 October 2023).

17. Exec. Order No. 14179, 'Removing Barriers to American Leadership in Artificial Intelligence' (23 January 2025).

C. Government and Institutional Materials (India)

18. NITI Aayog, National Strategy for Artificial Intelligence: #AIforAll (Government of India, June 2018).
19. NITI Aayog, Responsible AI for All: Approach Document for India, Part 1 – Principles for Responsible AI (February 2021).
20. NITI Aayog, Responsible AI for All: Approach Document for India, Part 2 – Operationalising Principles for Responsible AI (August 2021).
21. NITI Aayog, Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology (November 2022).
22. Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines (5 November 2025).
23. Ministry of Electronics and Information Technology, Advisory on Due Diligence by Intermediaries/Platforms regarding Artificial Intelligence (1 March 2024, superseded) and Revised Advisory (15 March 2024).
24. Ministry of Electronics and Information Technology, Draft Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 concerning Synthetically Generated Information (22 October 2025).
25. Press Information Bureau, Government of India, 'Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem' (7 March 2024).
26. Supreme Court of India, White Paper on Artificial Intelligence and the Judiciary (November 2025).
27. India AI Impact Summit 2026, Declaration (New Delhi, 16–21 February 2026).

D. Case Law

28. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
29. *Justice K.S. Puttaswamy (Aadhaar-5 J.) v. Union of India*, (2019) 1 SCC 1.
30. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

31. *Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd. & Anr.*, Civil Appeal No. 11950 of 2025 (Supreme Court of India, 2 July 2026).
32. *Gummadi Usha Rani & Anr. v. Sure Mallikarjuna Rao & Anr.* (Supreme Court of India, 2026).
33. *ANI Media Pvt. Ltd. v. OpenAI OpCo LLC* (Delhi High Court, 2025–26).
34. *State v. Loomis*, 2016 WI 68, 881 N.W.2d 749 (Wis. 2016).
35. *NJCM c.s. and FNV v. The State of the Netherlands* (SyRI), District Court of The Hague, ECLI:NL:RBDHA:2020:1878 (5 February 2020).
36. *R (Bridges) v. Chief Constable of South Wales Police*, [2020] EWCA Civ 1058.
37. *OQ v. Land Hessen* (SCHUFA Holding), Case C-634/21, Court of Justice of the European Union (7 December 2023).

E. Books and Scholarly Articles

38. Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999).
39. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015).
40. Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33(1) *International Review of Law, Computers & Technology* 76.
41. Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2021) 19(1) *International Journal of Constitutional Law* 41.
42. Edoardo Celeste and Giovanni De Gregorio, 'Digital Humanism: The Constitutional Message of the GDPR' (SSRN, 2022).
43. David Hadwick and Shimeng Lan, 'Lessons to Be Learned from the Dutch Childcare Allowance Scandal: A Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany' (2021) 13(4) *World Tax Journal* 609.

F. Reports and Online Sources

44. Royal Commission into the Robodebt Scheme, *Final Report* (Commonwealth of Australia, 2023).

45. Internet Freedom Foundation, legal notice to the National Crime Records Bureau concerning the Automated Facial Recognition System.
46. 'Explained: Delhi Police's AI surveillance network and why it's under scrutiny', The News Minute (2026).
47. 'Facial Recognition in India: Privacy, Surveillance and the Need for Regulation', amlegals (2026).
48. 'Indian courts have an AI problem, and the Supreme Court is not amused', The Federal (2026).
49. 'India's SC warns against unsupervised AI use in rulings', Law.asia (2026).
50. 'India's First AI Copyright Ruling: The Delhi High Court In ANI v. OpenAI', Mondaq (2026).
51. Council of the European Union, press releases on the Digital Omnibus package (May and June 2026).
52. Council of Europe, 'European Union ratifies the Council of Europe Framework Convention on Artificial Intelligence' (15 May 2026).