International Journal of
Law, Politics and Governance
ISSN: 3143-7028 | https://www.ioro.org/ijlpg

From Colonial Constitutionalism to Algorithmic Governance: The Evolution of Constitutional Freedom, Liberty and Human Dignity in India in the Age of Artificial Intelligence

A Comparative Study of India, the United States and China

Kunal Agarwal [1,*], Suryan Vats Upadhyaya [2], Neelabh Nayan Kalita [3]

[1] *LL.M., Amity University, Noida, Delhi NCR, India • agarwallakunal@gmail.com*

[2] *B.A. LL.B. Student, Centre for Juridical Studies, Dibrugarh, Assam, India • suryan2204@gmail.com*

[3] *LL.M., Royal Global University, Guwahati, Assam, India • neelabhnayank@gmail.com*

* **Corresponding author:** agarwallakunal@gmail.com

Abstract

In the past ten years, artificial intelligence (AI) has moved from the margins of policy to the centre of constitutional debate. Automated decision systems now shape welfare distribution, policing, credit scoring, content moderation and electoral communication, and courts and legislatures are asking whether inherited constitutional notions of liberty, equality and dignity can meaningfully apply to code. This paper traces India's constitutional journey from colonial subject state to rights-bearing republic and compares it with the markedly different experiences of the United States and the People's Republic of China. It then examines how each jurisdiction is reshaping its fundamental rights regime in response to algorithmic governance, through a comparative public law analysis across three themes: the institutional design of AI regulation, the approach of courts to algorithmic accountability, and the treatment of privacy and data protection. The paper presents India as a middle-ground state that adopts the American language of judicial review while building a centralised regulatory structure that resembles the Chinese model in form, though not in intent. Tables and figures are used throughout to visualise the comparative findings.

Keywords: algorithmic governance; human dignity; right to privacy; judicial review; data protection; comparative constitutional law

1. Introduction

Every constitution is written in response to a particular fear. The Indian Constitution is grounded in the experience of colonial rule and communal violence. The American Constitution was drafted in reaction to monarchical excess. The present Chinese Constitution was framed in the shadow of the Cultural Revolution and forms part of the Communist Party's continuing effort to direct the country's development. None of the three documents imagined a world in which decisions on welfare eligibility, employment, credit, speech and even the grant of bail would be made, or heavily influenced, by a statistical model trained on past data.

AI challenges constitutional law in a particular way. Classical constitutional guarantees assume a state actor, or occasionally a powerful private actor, whose conduct can be traced, reasoned about and challenged. The

© 2026 The Author(s). Published by IORO Publications. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/), which permits use, distribution, and reproduction in any medium, provided the original author and source are credited, a link to the license is provided, and any changes are indicated.

algorithm complicates each of these assumptions. It is difficult to know how it works, how it is used and what it does to the person it affects, sometimes even for its own creators, and its impact is often not apparent to the affected person until after the decision has been made. The result is a widening gap between the constitutional rights that citizens hold and their practical ability to assert those rights against automated power, whether exercised by the state or by private platforms acting with state complicity.

The paper is organised as follows. Section 2 gives a historical account of the development of constitutionalism in India, the United States and China, explaining the different paths that produced the present balance between state power and individual liberty in each country. Section 3 examines how the doctrine of fundamental rights, and the value of human dignity, has been redefined in response to automated governance. Sections 4, 5 and 6 undertake the comparative public law study proper: the architecture of AI regulation, the role of judicial interpretation in algorithmic accountability, and the regulation of data protection and surveillance. Section 7 sets out the findings, and Section 8 concludes with modest recommendations for Indian law and policy.

The method is doctrinal and comparative. The paper draws on constitutional texts, case law, current and recently published statutes and delegated legislation in each jurisdiction, and secondary academic and policy literature. Because this is one of the most rapidly changing areas of regulation, care has been taken to record the legal position in each country as it stands in 2026, while recognising that further changes are likely.

2. The Historical Evolution of Constitutionalism in India, the United States and China

2.1. India: From Colonial Subjecthood to Constitutional Citizenship

The colonial prehistory is integral to understanding constitutionalism in India. The Government of India Acts of 1858, 1919 and 1935[1] were instruments of imperial rule, not charters of liberty. They divided power between the Viceroy and limited representative bodies, but they did not recognise the Indian population as citizens in any real sense. Civil liberties, to the extent they existed, rested on statute and could be withdrawn by executive notification, as the repeated use of preventive detention laws against the independence movement showed. The framers of the Indian Constitution (1946 to 1949) were acutely aware of this history, and the fundamental rights in Part III of the Constitution[2] were drafted in direct response to colonial arbitrariness.

As originally framed, Article 21 provided that “no person shall be deprived of his life or personal liberty except according to procedure established by law”. In *A.K. Gopalan v. State of Madras*,[3] the Supreme Court treated the fundamental rights as watertight compartments and asked only whether a formal procedure existed, not whether that procedure was fair. This narrow reading prevailed until *Maneka Gandhi v. Union of India*,[4] decided after the Emergency, which read a requirement of fair, just and reasonable procedure into Article 21 and connected it with Articles 14 and 19. The Emergency of 1975 to 1977, during which citizens' right to move the courts for the enforcement of personal liberty was suspended, remains the gravest warning in Indian constitutional history. It still weighs on judges whenever they are asked to dilute constitutional safeguards by granting the executive unchecked power, even where that power is exercised through automation.

[1] Government of India Act, 1858 (21 & 22 Vict. c. 106); Government of India Act, 1919 (9 & 10 Geo. 5 c. 101); Government of India Act, 1935 (26 Geo. 5 c. 2).

[2] The Constitution of India, 1950, pt. III, arts. 12-35.

[3] *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27.

[4] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

In *Kesavananda Bharati v. State of Kerala*[5] and *Minerva Mills Ltd. v. Union of India*,[6] the basic structure doctrine placed limits on Parliament's amending power, holding that fundamental rights and judicial review form part of the basic structure of the Constitution and cannot be abrogated even by constitutional amendment. The doctrine is directly relevant to algorithmic governance: it is the basis for the principle that no future Parliament may simply legislate away judicial control over automated state action.

The most significant recent development is the recognition of privacy as a fundamental right. In 2017, a nine-judge bench of the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*[7] unanimously held that the right to privacy is protected under Part III of the Constitution and is an intrinsic part of the right to life and personal liberty under Article 21. Significantly, the judgment repudiated the reasoning of the Emergency-era decision in *ADM Jabalpur v. Shivkant Shukla*,[8] which had held that the right to personal liberty could be suspended, and grounded privacy in the wider constitutional value of dignity. A second *Puttaswamy* decision in 2018[9] tested the Aadhaar biometric identification scheme against this newly recognised right. The Court upheld the scheme's basic architecture but struck down mandatory linking of Aadhaar with bank accounts and mobile connections, as well as the extension of the scheme to private entities. Together, the two *Puttaswamy* decisions form the constitutional bedrock on which India's later debates on data protection, and now on AI governance, rest.

2.2. The United States: The Liberal Constitutional Tradition and the Administrative State

The American constitutional tradition begins from a different premise. Conceived in the aftermath of British rule, the Constitution was designed to limit and separate governmental power, and the Bill of Rights, adopted in 1791, served as a key check on federal encroachment on individual liberty. Judicial review is not expressly provided for in the text, but was established by the Supreme Court in *Marbury v. Madison*,[10] which held that the Court may strike down legislative or executive action that is unconstitutional. The case laid the foundation for the independent judiciary that defines American public law, including its power to set aside automated government decision-making.

Two strands of American constitutional history are especially significant for AI. The first is the Fourth Amendment tradition on search and seizure, which has repeatedly had to adapt to new surveillance technology. *Katz v. United States*[11] abandoned a narrow property-based notion of search in favour of a reasonable expectation of privacy standard. More recently, in *Carpenter v. United States*,[12] the Court held that cell-site location records generated by mobile phones provide a comprehensive record of a person's movements, so that accessing them is a search requiring a warrant. *Carpenter* is widely read as a sign of the judiciary's willingness to extend constitutional protection into the data-driven world on which AI systems depend.

The second strand concerns the rise of the administrative state and the constraints on agencies that rely on automated decision-making. American courts have used the doctrine of procedural due process to question algorithmic tools in the administration of public benefits and in criminal sentencing. The Wisconsin Supreme

[5] *Kesavananda Bharati v. State of Kerala*, (1973) 4 SCC 225.

[6] *Minerva Mills Ltd. v. Union of India*, (1980) 3 SCC 625.

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

[8] *Additional District Magistrate, Jabalpur v. Shivkant Shukla*, (1976) 2 SCC 521.

[9] *Justice K.S. Puttaswamy (Aadhaar-5 J.) v. Union of India*, (2019) 1 SCC 1.

[10] *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).

[11] *Katz v. United States*, 389 U.S. 347 (1967).

[12] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

Court's decision in *State v. Loomis*[13] is a bold but measured precedent. The court permitted the use of the proprietary risk assessment tool COMPAS at sentencing, but required that its use be accompanied by written warnings about the tool's limitations, leaving open the constitutional question whether the state may rely on opaque proprietary algorithms at all. Unlike India and China, the United States has no single overarching federal law on AI or on data protection generally. Its federal design has instead produced a patchwork of state laws, discussed further in Section 4.

2.3. China: From Dynastic Governance to Socialist Constitutionalism with Chinese Characteristics

China's constitutional trajectory departs fundamentally from both the Indian and American paths. The current Constitution, adopted in 1982 and amended several times since, including a significant 2004 amendment inserting into Article 33 the statement that the state respects and safeguards human rights, operates within a one-party socialist system in which the Constitution does not function as a source of judicially enforceable individual rights against the state in the manner familiar to Indian or American lawyers. Ordinary courts in China do not exercise the power of constitutional review over legislation. That function, to the extent it exists at all, is reserved to the National People's Congress and its Standing Committee, organs of the same party-led system that enacts the legislation in question.

This does not mean that Chinese public law is indifferent to individual interests. Rather, protection of interests such as privacy, reputation and personal data has developed primarily through ordinary legislation, most importantly the Cybersecurity Law of 2017, the Civil Code of 2020, the Data Security Law of 2021 and the Personal Information Protection Law of 2021,[14] rather than through constitutional adjudication. These statutes create administrative and civil remedies enforced by regulators such as the Cyberspace Administration of China, rather than a body of constitutional case law comparable to *Puttaswamy* or *Carpenter*. The absence of independent judicial review of legislation is a structural feature, not an oversight, and it shapes every comparison in this paper. Where India and the United States rely on courts to test executive and legislative action against a bill of rights, China relies on the Communist Party and state administrative organs to calibrate the balance between technological development, social stability and individual interest, a model its own scholarship describes as governance through law rather than government under a rights-based constitution enforced by an independent judiciary.

2.4. A Comparative Overview

Table 1 summarises the structural differences in constitutional design that condition each jurisdiction's response to AI.

Table 1. Comparative constitutional design.

Feature	India	United States	China
Constitutional foundation	Constitution of India, 1950	Constitution of the United States, 1787 (in force 1789)	Constitution of the People's Republic of China, 1982, as amended
Source of fundamental rights	Part III, Articles 12 to 35	Bill of Rights (Amendments I to X) and the Fourteenth Amendment	Chapter II, Articles 33 to 56
Judicial review of legislation	Yes, entrenched through the basic structure doctrine (*Kesavananda Bharati*, 1973)	Yes, established in *Marbury v. Madison* (1803)	No independent judicial review of legislation; oversight rests with the NPC Standing Committee

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

[14] Cybersecurity Law of the People's Republic of China (2017); Civil Code of the People's Republic of China (2020); Data Security Law of the People's Republic of China (2021); Personal Information Protection Law of the People's Republic of China (2021).

Feature	India	United States	China
Formative constitutional crisis	Colonial rule; the Emergency of 1975 to 1977	The struggle against monarchical and colonial authority	The Cultural Revolution and the reform and opening era after 1978
Dominant rights value in current doctrine	Human dignity, as elaborated after *Puttaswamy* (2017)	Liberty and procedural due process	Social stability and collective welfare, alongside a textual human rights guarantee in Article 33

Fig. 1 places the three jurisdictions on a single timeline, showing how constitutional milestones and AI-specific regulatory milestones have interacted over the last decade.

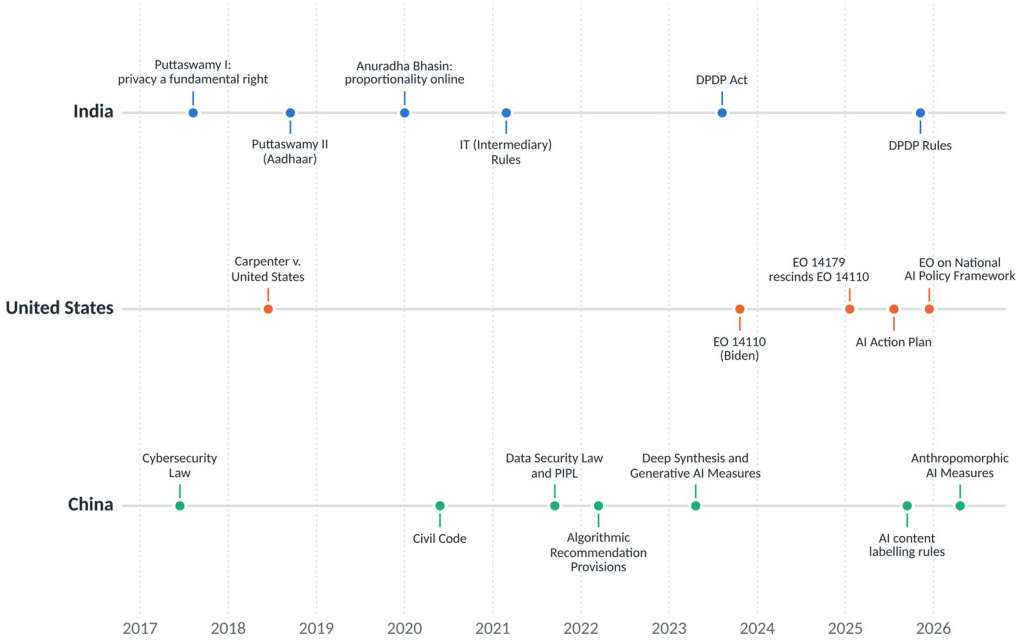


Fig. 1. Comparative timeline of constitutional and AI governance milestones, 2017 to 2026.

3. Fundamental Rights, Liberty and Human Dignity in the Algorithmic Age

3.1. India: Dignity as the Organising Constitutional Value

The *Puttaswamy* ruling did more than recognise a distinct right to privacy. It elevated human dignity to a foundational value underpinning the entire constitutional order. Once dignity, and not mere legality, becomes the measure by which state action may be invalidated, the allocation of benefits or entitlements through automated eligibility determinations risks not just administrative error but constitutional injury. This dignity-centred reasoning has already produced case law whose contours are useful in the algorithmic governance context. In *Anuradha Bhasin v. Union of India*,[15] decided in 2020, the Court held that internet access is integral to the exercise of several fundamental rights and that any restriction on connectivity must satisfy the test of proportionality. Proportionality, a doctrine borrowed by Indian courts from comparative constitutional law, has since become the primary framework for assessing the legality of digital restrictions, and it will almost certainly be the analytical lens applied to future challenges to opaque algorithmic decision-making by the state.

[15] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

Earlier, in *Shreya Singhal v. Union of India*,[16] the Court had struck down Section 66A of the Information Technology Act[17] as unconstitutionally vague, at a time when the state was still settling the boundaries of internet regulation. The decision is frequently cited in current debates on regulating AI platforms. The Digital Personal Data Protection Act, 2023, now operationalised by the DPDP Rules, 2025 after a lengthy consultation, is the statutory embodiment of the *Puttaswamy* principle. On publication, however, civil society groups such as the Internet Freedom Foundation observed that its architecture is heavily oriented towards facilitating data processing by the state, for governance as well as commercial purposes.

3.2. The United States: Liberty, Due Process and the Limits of a Negative Rights Tradition

In its classical interpretation, the American Bill of Rights is a negative rights document. It restrains government from acting rather than requiring it to act, and under the state action doctrine it binds government actors rather than private ones. This creates a particular difficulty for algorithmic governance, because the AI systems that most affect the daily lives of ordinary Americans, such as content recommender systems, hiring screens, credit scoring models and insurance pricing tools, are usually operated by private rather than state actors, and due process and equal protection do not, without more, apply to purely private conduct. Where the government itself operates an automated regime, however, due process doctrine has begun to keep pace. Courts and administrative tribunals have required that persons affected by automated benefit denials and algorithmic risk scores receive notice, an opportunity to challenge the decision, access to the evidence and a chance to present a defence. This approach, long established for welfare terminations in *Goldberg v. Kelly*,[18] has now been extended by analogy to automated decision systems.

It was therefore unsurprising that a federal administration intent on establishing a “minimally burdensome national policy” would, in December 2025, issue an executive order setting out a national policy framework for AI and creating an AI Litigation Task Force within the Department of Justice to challenge state AI laws. Federalism, rather than any settled theory of individual rights, is now the central arena in which the scope of AI regulation in the United States is being decided.

3.3. China: Human Dignity within a Governance Framework

The 2004 amendment to the Chinese Constitution,[19] which added an express commitment to respecting and safeguarding human rights to Article 33, together with the Article 38 guarantee that the personal dignity of citizens is inviolable, provides a textual basis for dignity as a value in Chinese public law. In practice, however, there is no strong tradition of constitutional litigation, and the overwhelming bulk of positive protection for citizens' dignity interests against algorithmic harm comes from statute and regulation rather than constitutional adjudication. The Personal Information Protection Law of 2021 does contain legally enforceable rights closely resembling those in the European General Data Protection Regulation and India's DPDP Act, including rights of access, correction and deletion, and, under Article 24,[20] a right to request an explanation of automated decisions and to refuse decisions made solely by automated means.

Through the Algorithmic Recommendation Provisions of 2022, the Deep Synthesis Provisions of 2023 and the Interim Measures for the Management of Generative AI Services, effective August 2023,[21] China's regulation

[16] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

[17] Information Technology Act, 2000, s. 66A (struck down in *Shreya Singhal v. Union of India*, (2015) 5 SCC 1).

[18] *Goldberg v. Kelly*, 397 U.S. 254 (1970).

[19] Constitution of the People's Republic of China, 1982 (as amended 2004), art. 33.

[20] Personal Information Protection Law of the People's Republic of China (2021), art. 24.

[21] Provisions on the Administration of Algorithm-Generated Recommendations for Internet Information Services (2022); Provisions on the Administration of Deep Synthesis Internet Information Services (2023); Interim Measures for the Management of Generative Artificial

of algorithmic and generative systems imposes duties on content, algorithmic design and training data comparable to the content and platform governance undertaken by Western law. These include duties to prevent discrimination in algorithmic design and training data, duties to protect the legitimate rights and interests of individuals, including dignity and reputation, and, from September 2025, mandatory labelling of AI-generated content. The limit of this state-directed model is that individuals may pursue these interests only through administrative complaints or, since the 2020 Civil Code, through civil proceedings against the service provider concerned. They cannot assert these rights against the state directly in court so as to have an administrative regulation set aside.

3.4. Comparative Reflection

This part offers a qualitative, doctrinally based comparison of the three systems on the dimensions the authors consider most relevant: the degree of centralisation in AI rule-making, the availability of independent judicial review of algorithmic harms, the strength of the statutory data protection framework, the protection of free expression online, and the extent of executive discretion retained in each system. The assessment in Fig. 2 reflects the authors' doctrinal judgment on the legal materials discussed in this paper. It is offered as an aid to interpreting the doctrine and not as an empirical measurement.

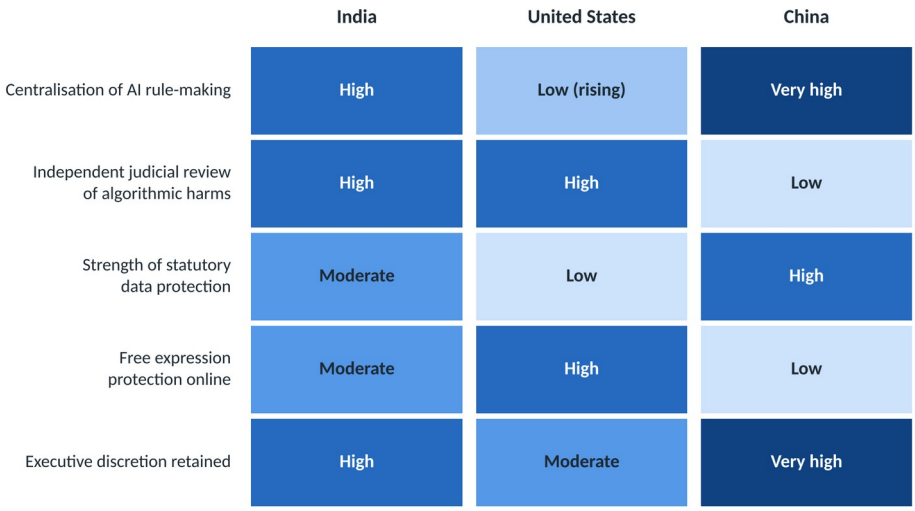


Fig. 2. Doctrinal assessment of algorithmic governance models. The ratings are the authors' qualitative judgment based on the legal materials discussed in this paper, not an empirical measurement.

The picture that emerges is one of genuine divergence beneath a surface convergence of vocabulary. All three jurisdictions now speak of transparency, accountability, non-discrimination and data protection in their AI-related instruments. The institutional guarantees behind that vocabulary, however, differ sharply, a theme explored in the remaining sections of this paper.

4. Comparative Public Law Study I: Institutional and Regulatory Architecture for Algorithmic Governance

The first theme of the comparative public law study is institutional design: what form a legal system of AI regulation should take. The question lies squarely within administrative and constitutional law, since it determines who holds power over AI and to whom that power is accountable.

Intelligence Services (2023).

Indian regulation follows a sectoral model layered on top of a general data protection law. The Ministry of Electronics and Information Technology is the nodal ministry for digital governance. It framed the Information Technology Rules, 2021[22] for intermediaries and digital media and has steered the DPDP Act and Rules to notification. Both NITI Aayog's earlier strategy papers on responsible AI and the Ministry's recent AI governance guidelines adopt a light-touch, innovation-friendly approach, with no horizontal AI law of the kind enacted in the European Union. The 2025 Rules operationalise the Data Protection Board of India as an executive body with adjudicatory powers over data protection matters, with appeals lying to the Telecom Disputes Settlement and Appellate Tribunal rather than to a specialised AI regulator. In institutional terms, the Indian model is a hybrid between the sector-specific approach favoured in the United States and the "one-stop shop" model favoured in Europe and China, coupled with significant executive discretion, including the central government's broad rule-making and exemption powers under the DPDP Act.

Unlike India, the United States has no single regulator for AI or data protection. Authority is spread across sectoral agencies with jurisdiction over AI-related practices, such as the Federal Trade Commission (FTC) in respect of unfair or deceptive practices and financial regulators in respect of algorithmic credit decisions under existing fair lending law, with executive policy shifting through executive orders. In October 2023, President Biden issued Executive Order 14110,[23] directing federal agencies to develop guidance to ensure that AI systems are safe and protect rights. In January 2025, President Trump rescinded that order through Executive Order 14179,[24] adopting a more deregulatory stance that was carried forward in the AI Action Plan of July 2025 and in the December 2025 executive order directing the Attorney General to establish an AI Litigation Task Force to challenge state AI laws considered unduly restrictive. The result is a highly fluid institutional landscape in which a federal model that coordinated policy in the name of rights has, within three years, been replaced by an explicitly deregulatory one, while the underlying constitutional question, essentially one of federalism, is now before the courts.

China's model is the most centralised of the three. The Cyberspace Administration of China is the lead regulator, coordinating with other bodies such as the National Development and Reform Commission, the Ministry of Industry and Information Technology and the Ministry of Public Security. In rapid succession it has issued the Algorithmic Recommendation Provisions, the Deep Synthesis Provisions, the Generative AI Measures and, most recently, the Anthropomorphic AI Interaction Services Measures, promulgated in April 2026 and effective from July 2026. This framework enables a prompt and coordinated regulatory response, illustrated by the mandatory content labelling rules introduced in September 2025 and by the Cyberspace Administration's active enforcement, including taking unregistered generative AI applications offline. It also confers wide discretion on administrative officials and offers little or no means for a regulated entity or an affected individual to challenge the substance of a rule before a court, as opposed to the manner of its application.

Table 2 sets out the principal regulatory instruments currently in force or recently promulgated in each jurisdiction, permitting a side-by-side comparison of institutional design.

Table 2. Comparative regulatory instruments for AI governance.

[22] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

[23] Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

[24] Exec. Order No. 14,179, 90 Fed. Reg. 8741 (Jan. 23, 2025).

Jurisdiction	Lead Institutions	Key Instruments (current as of 2026)	Predominant Legal Form
India	Ministry of Electronics and Information Technology; Data Protection Board of India	Digital Personal Data Protection Act, 2023; DPDP Rules, 2025; Information Technology Rules, 2021; NITI Aayog papers on Responsible AI	Statute, delegated legislation and policy guidance
United States	Federal Trade Commission and sectoral agencies; Office of Science and Technology Policy; state legislatures	Executive Order 14179 (2025); America's AI Action Plan (July 2025); Executive Order on a National AI Policy Framework (December 2025); state statutes such as the CPRA, the Colorado AI Act and the Illinois BIPA	Executive order and state statute; no dedicated federal AI or privacy statute
China	Cyberspace Administration of China, coordinating with the NDRC, the Ministry of Industry and Information Technology and the Ministry of Public Security	Cybersecurity Law, 2017; Data Security Law and Personal Information Protection Law, 2021; Algorithmic Recommendation Provisions, 2022; Deep Synthesis Provisions, 2023; Generative AI Measures, 2023; Anthropomorphic AI Interaction Services Measures, 2026	Statute and coordinated administrative regulation

5. Comparative Public Law Study II: Judicial Review and Algorithmic Accountability

The second theme is the approach of courts to algorithmic decision-making, which engages the separation of powers in each jurisdiction. Indian courts have not yet confronted a case in which a particular AI system is tested for constitutionality, but the doctrinal tools are already in place. The four-part proportionality standard articulated in *Puttaswamy* and applied in *Anuradha Bhasin* requires that a measure pursue a legitimate aim, be suitable and necessary to achieve it, and strike a proper balance between the right and the competing public interest. It is well suited to scrutinising automated welfare exclusion, predictive policing and facial recognition once these are litigated. Unlike in China, an aggrieved individual in India has a constitutional route to challenge the state's use of an algorithmic system, through the writ jurisdiction of the High Courts under Article 226 and of the Supreme Court under Article 32. Principles of Indian administrative law, notably the duty to give reasons and the requirements of natural justice, have been invoked to seek explainability of automated government systems, although no reported Indian judgment has yet reached the merits of that argument.

With a more established tradition of judicial scrutiny dating back to *Marbury v. Madison*,[25] American courts have engaged more directly, if cautiously, with algorithmic tools. *Loomis*[26] remains the paradigm case. Its willingness to overlook the proprietary nature of a risk assessment algorithm as a due process violation, provided adequate cautionary disclosures accompany its use, has drawn sustained academic criticism for permitting a degree of algorithmic opacity to persist in the criminal justice system. *Carpenter*[27] reflects a far more protective stance towards individual liberty in the face of the volume and comprehensiveness of data that digital systems generate about a person's life, and its reasoning has shaped subsequent lower court rulings on geofence warrants and other AI-adjacent law enforcement tools. In the common law manner, American doctrine develops incrementally, case by case, rather than from a comprehensive prior theory of algorithmic governance.

[25] *Marbury v. Madison*, *supra* note 10.

[26] *State v. Loomis*, *supra* note 13.

[27] *Carpenter v. United States*, *supra* note 12.

As noted in Section 2, Chinese courts do not undertake constitutional review of laws or of the administrative regulations of the Cyberspace Administration of China. Judicial involvement in algorithmic accountability in China takes two other forms: administrative litigation against the application of a rule in a particular case, and civil litigation founded on the personality rights provisions of the Civil Code and the private right of action for unlawful processing under the Personal Information Protection Law. Courts have already decided several civil cases concerning facial recognition and algorithmic price discrimination under these statutory causes of action, offering a narrower but valuable avenue for relief that does not challenge the limits that legislators and regulators have set for these technologies. This is the clearest structural difference among the three jurisdictions: in India and the United States, a court may review the algorithmic governance scheme itself against a higher constitutional standard; in China, it may not.

6. Comparative Public Law Study III: Data Protection, Privacy and Surveillance in the Algorithmic Age

The third theme is data protection and surveillance, the substantive area in which most current disputes over AI arise and in which most regulation is actually taking place. Access to personal data is the raw material of most contemporary algorithms and the channel through which most algorithmic harm reaches individuals.

In India, the Digital Personal Data Protection Act, 2023, together with the 2025 Rules,[28] adopts a consent-based framework and aims at simple, accessible, rational and actionable regulation. It requires data fiduciaries to give clear notice, obtain informed consent, appoint a Data Protection Officer in the case of significant data fiduciaries, and report personal data breaches to the newly established Data Protection Board within prescribed timelines. The Act also contains wide exemptions for processing by the state, including processing that may feed AI systems used for surveillance or welfare administration, and processing in the interests of sovereignty, security and public order, which is not subject to the consent and purpose limitation safeguards that bind private fiduciaries. The tension between a fundamental right to privacy under the Constitution and a broad statutory grant of immunity to the state is likely to become the focus of Indian AI and data protection litigation in the coming years.

The United States has no federal law comparable to the DPDP Act or China's Personal Information Protection Law. Constitutional privacy protection continues to rest on Fourth Amendment search and seizure doctrine, which applies only to government action and, after *Carpenter*, has meaningful effect on digital records only where a comparably comprehensive picture of private life is involved. In the private sector, where most AI training and deployment takes place, the field is governed by a patchwork of sectoral federal statutes, such as the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act and the Fair Credit Reporting Act, with state comprehensive privacy laws unevenly filling the gaps. As a result, the protection available to a data subject against algorithmic profiling in the United States depends heavily on the state and the sector, and that patchwork is now directly targeted by the federal preemption measures launched in December 2025.

In certain technical respects, China's data protection framework, comprising the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law, is the most comprehensive of the three. Data localisation requirements for critical information infrastructure operators, restrictions on cross-border transfers and the right under Article 24 of the Personal Information Protection Law to refuse solely automated decisions are examples. Enforcement is strict, with substantial administrative fines under the Personal Information Protection Law calculated, as under the European Union's General Data Protection

[28] The Digital Personal Data Protection Act, 2023 (India); Digital Personal Data Protection Rules, 2025 (India).

Regulation, as a percentage of annual turnover. The framework, however, is subordinate to the larger goals of national security and social stability. While it restrains private companies, it leaves the state considerable room to collect and use personal data for public security purposes with comparatively little external check. This is broadly the inverse of the American position, in which private companies may collect and use personal data with comparatively little restriction, while public authorities face constitutional constraints under the Fourth Amendment.

Table 3 offers a comparative snapshot of the data protection and surveillance regimes of the three jurisdictions.

Table 3. Comparative data protection and surveillance regimes.

Feature	India	United States	China
Governing instrument	DPDP Act, 2023 and DPDP Rules, 2025	Sectoral federal statutes (HIPAA, GLBA, COPPA, FCRA) and state comprehensive privacy laws	Cybersecurity Law; Data Security Law; Personal Information Protection Law, 2021
Consent standard	Informed, purpose-specific consent, subject to broad state exemptions	Varies by sector and by state; no uniform national standard	Separate, specific consent under Article 14 of the PIPL, subject to state exemptions
Rights over automated decision-making	Not separately codified in the DPDP Act	No general federal right; limited sectoral and state provisions	Right to an explanation and to refuse solely automated decisions under Article 24 of the PIPL
Government access to personal data	Subject to the *Puttaswamy* proportionality standard, alongside broad statutory exemptions for the state	Subject to a Fourth Amendment warrant requirement following *Carpenter v. United States*	Extensive, with a national security and public order override
Principal enforcement body	Data Protection Board of India	Federal Trade Commission and state Attorneys General	Cyberspace Administration of China

7. Findings

Three findings emerge from this comparative study. First, the presence or absence of independent judicial review of legislation is the most important factor shaping how AI governance operates in practice, more so than the details of any governing statute. India and the United States have distinct rights traditions, but both entrust courts with the power to review the constitutional validity of algorithmic governance schemes, including statutory data protection provisions. China's courts, however active they may prove in enforcing statutory data protection rights, have no power to review the underlying regulatory framework against a higher constitutional standard.

Second, all three jurisdictions show a trend towards greater centralisation of executive power over AI policy, though for very different reasons. India's DPDP Act and Rules vest significant rule-making and exemption powers in the central government. The United States, historically a decentralised sectoral and federal system, is witnessing an aggressive executive effort to consolidate AI policy-making in Washington, D.C. and to pre-empt state regulation. China's model was centralised from the outset. This shift towards executive centrality deserves closer study, even in jurisdictions with a long tradition of judicial review, because it suggests that AI may increasingly be governed in practice through administrative rule-making rather than through constitutional design.

Third, human dignity, which appears in some form in each of the three constitutional traditions, performs very different doctrinal functions in each. In India, judicial interpretation has turned dignity into a rights-based

organising principle from which other rights, such as privacy, are derived. In the United States, dignity is less prominent in doctrine than in academic writing and is still handled largely through the lenses of due process and equal protection. In China, dignity is constitutionally guaranteed but realised primarily through statute and administrative regulation rather than adjudication. Because it is judicially enforceable, India's dignity-centred approach is the most promising of the three. It is also the most demanding, since the gap between the DPDP Act's sweeping state exemptions and the *Puttaswamy* standard has yet to be addressed, whether by the courts or through legislative reform.

8. Conclusion

The history of Indian constitutionalism is a history of building institutional distrust of unchecked power into the design of the state itself, a lesson learned first under colonial rule and then reinforced by the Emergency. That inheritance places India in an unusual position as AI reshapes the practical exercise of state and private power. Through *Puttaswamy* and the broader fundamental rights jurisprudence built on *Maneka Gandhi*, *Kesavananda Bharati* and *Anuradha Bhasin*, India possesses a constitutional vocabulary at least as rich as the American tradition for testing algorithmic governance against liberty and dignity. At the same time, India's regulatory instinct, expressed through the DPDP Act and Rules, has borrowed institutional features such as broad executive rule-making power, wide state exemptions and a centralised adjudicatory board, which sit closer to the Chinese model of administrative governance than to the fragmented, court-centred American approach.

This hybrid position is not necessarily a weakness. It may allow India to combine the coordinated, relatively fast-moving regulatory capacity that centralised systems such as China's demonstrate with the individual constitutional recourse that only an independent judiciary, of the kind India and the United States share, can provide. Whether India realises this potential will depend on decisions not yet made: chiefly, whether Indian courts, when finally confronted with a concrete algorithmic governance dispute, apply the proportionality standard of *Puttaswamy* and *Anuradha Bhasin* to automated state action with the same rigour they have applied to more conventional restrictions on liberty, and whether the broad exemptions available to the state under the DPDP Act are narrowed through future litigation or amendment. The comparative evidence assembled in this paper suggests that the answer to that question will determine, more than any single piece of legislation, whether India's constitutional commitment to liberty and human dignity survives its transition into the algorithmic age.

Funding

This research received no external funding.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

No new data were created or analysed in this study. All materials relied upon are publicly available legal sources cited in the footnotes.

AI Usage Disclosure

[To be completed by the authors.]

Author Contributions

[To be completed by the authors using CRediT roles.]

References

[1] The Constitution of India, 1950.

[2] Constitution of the United States, 1787.

[3] Constitution of the People's Republic of China, 1982 (as amended).

[4] Government of India Act, 1858; Government of India Act, 1919; Government of India Act, 1935.

[5] *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27.

[6] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

[7] *Kesavananda Bharati v. State of Kerala*, (1973) 4 SCC 225.

[8] *Minerva Mills Ltd. v. Union of India*, (1980) 3 SCC 625.

[9] *Additional District Magistrate, Jabalpur v. Shivkant Shukla*, (1976) 2 SCC 521.

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

[11] *Justice K.S. Puttaswamy (Aadhaar-5 J.) v. Union of India*, (2019) 1 SCC 1.

[12] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

[13] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

[14] *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).

[15] *Katz v. United States*, 389 U.S. 347 (1967).

[16] *Goldberg v. Kelly*, 397 U.S. 254 (1970).

[17] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

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

[19] Information Technology Act, 2000 (India).

[20] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

[21] The Digital Personal Data Protection Act, 2023 (India); Digital Personal Data Protection Rules, 2025 (India).

[22] Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

[23] Exec. Order No. 14,179, 90 Fed. Reg. 8741 (Jan. 23, 2025).

[24] Cybersecurity Law of the People's Republic of China (2017); Civil Code of the People's Republic of China (2020); Data Security Law of the People's Republic of China (2021); Personal Information Protection Law of the People's Republic of China (2021).

[25] Provisions on the Administration of Algorithm-Generated Recommendations for Internet Information Services (2022); Provisions on the Administration of Deep Synthesis Internet Information Services (2023); Interim Measures for the Management of Generative Artificial Intelligence Services (2023).