Naveen Shodh Sansar (An International Refereed / Peer Review Multidisciplinary Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 8.054,
July to September 2025, E-Journal, Vol. I, Issue LI (51), ISO 9001:2015 - E2024049304 (QMS)

# AI Governance and Constitutional Accountability in India: A Critical Analysis

**Rishabh Bhan Singh* Prof. (Dr.) Anand Paliwal****

*Research Scholar (Law) MLSU, Udaipur (Raj.) INDIA
** Department of Law, MLSU, Udaipur (Raj.) INDIA

**Abstract:**This paper examines whether India's current and emerging artificial intelligence governance frameworks satisfy the requirements of constitutional accountability under Part III of the Constitution of India. Employing a doctrinal and comparative methodology, the paper analyses the application of Articles 14, 19, and 21 — including the doctrines of non-arbitrariness, proportionality, and procedural due process — to algorithmic decision-making by the Indian State. It argues that the Constitution, as judicially elaborated through decisions including Justice K.S. Puttaswamy v. Union of India (2017) and Anuradha Bhasin v. Union of India (2020), provides a substantially adequate normative framework for governing AI, but that the existing regulatory architecture — comprising the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and non-binding policy instruments — is structurally inadequate to operationalise that framework. Drawing on comparative analysis of the European Union's AI Act and the United States' sectoral approach, the paper proposes constitutionally grounded reforms including comprehensive AI legislation, mandatory algorithmic impact assessments, an independent regulatory authority, and the judicial recognition of a constitutional right to explanation for consequential algorithmic decisions.

**Introduction -** The Indian State is deploying artificial intelligence across its core governance functions at a pace that substantially outstrips the development of any corresponding legal framework. The Aadhaar biometric authentication system, mediating access to food rations for approximately 800 million persons, relies on algorithmic deduplication and matching.[1] Facial recognition technology has been deployed by police forces in over thirty locations across India without specific statutory authorisation.[23] The Faceless Assessment Scheme in income tax administration incorporates algorithmic risk-scoring for case selection. The Supreme Court Portal for Assistance in Courts' Efficiency (SUPACE) introduces AI-assisted research into the judicial function itself. Each deployment engages constitutional commitments of the highest significance: equality, liberty, privacy, due process, and the rule of law.

This paper addresses a specific research question: does India's current AI governance framework satisfy the requirements of constitutional accountability derived from Part III of the Constitution? The thesis advanced is twofold. First, that the Constitution of India, as judicially elaborated through seven decades of sustained interpretive development, provides a substantially adequate normative framework for disciplining algorithmic state action — the doctrinal resources exist and need not be invented. Second, that what is lacking is the operational, statutory, and institutional architecture necessary to translate that doctrine into the governance of specific AI deployments. The gap between constitutional doctrine and operational governance constitutes the defining challenge of AI regulation in India. The methodology is doctrinal and comparative. The doctrinal component applies established constitutional tests — the classification doctrine and non-arbitrariness principle under Article 14,[4] the Shreya Singhal standard under Article 19,[5] and the proportionality framework under Article 21[6] — to the specific characteristics of algorithmic systems. The comparative component examines the European Union's AI Act[7] and the United States' sectoral approach as heuristic reference points. The paper does not argue for uncritical transposition of foreign models; it argues for the development of an Indian architecture grounded in Indian constitutional commitments.

**Theoretical Framework: AI Governance, Rule Of Law, And Constitutional Accountability:** Constitutional accountability, as deployed in this paper, denotes the obligation of the State to exercise public power — including algorithmic power — in a manner that is transparent, justifiable, and subject to effective review. It encompasses both vertical accountability (the answerability of the State to citizens through judicial and democratic mechanisms) and horizontal accountability (the mutual checks exercised by constitutional organs upon one another). When the State deploys an AI system that determines welfare eligibility, identifies criminal suspects, or modulates access to

information, constitutional accountability demands that the deployment be authorised by law, proportionate to a legitimate aim, and amenable to meaningful judicial review. Algorithmic governance generates distinctive challenges to constitutional accountability that the existing literature has identified with increasing precision. Pasquale's foundational analysis of the "black box" character of algorithmic systems demonstrates that consequential decisions are increasingly made through processes that are structurally opaque to those they affect.[8] Hildebrandt has argued that the "computational turn" in governance requires not merely the application of existing law to new objects but a structural reconfiguration of the law-technology relationship.[9] Citron has identified the concept of "technological due process" — the argument that constitutional safeguards must be embedded at the design stage of algorithmic systems rather than applied exclusively through post-deployment judicial review.[10] Balkin has examined how the rise of "big data" transforms the relationship between citizens and the State, arguing for fiduciary-like obligations on entities that control consequential data flows.[11]

These scholarly interventions converge on a central insight: the deployment of AI in governance is not merely a technological development to which law must react; it is a transformation in the modality of state power that engages constitutional commitments at the most fundamental level. The rule of law — identified by the Supreme Court as a basic structure component in S.R. Bommai v. Union of India (1994) — requires that state action proceed from identifiable legal authority, be exercisable only through fair and transparent procedures, and be subject to independent review. AI-mediated state action that operates without statutory foundation, through inscrutable computational processes, and without effective mechanisms for challenge fails each of these requirements.

**The Existing AI Governance Framework In India: A Critical Assessment**

**A. The Policy-Legislation Gap:** India's AI governance regime is characterised by a fundamental structural asymmetry: substantial policy articulation coupled with minimal legislative operationalisation. The NITI Aayog's National Strategy for Artificial Intelligence (2018) identified AI as a transformative technology and articulated developmental priorities.[12] The Responsible AI for All framework (2021) enumerated seven principles — safety, equality, non-discrimination, privacy, transparency, accountability, and human values — that are substantively sound and consistent with international best practice.[13] The MeitY Sub-Committee on AI Governance (2024) acknowledged the structural limitations of existing legislation and proposed more comprehensive engagement.[14]

These instruments, however, occupy the domain of soft law — they articulate principles without creating binding obligations, enforcement mechanisms, or remedial avenues. The gap between principle and implementation is constitutional. The Supreme Court's consistent requirement — from Gobind v. State of Madhya Pradesh (1975) through PUCL v. Union of India (1997)[15] to Puttaswamy (2017)[16] — is that measures restricting fundamental rights be sanctioned by law, not merely by policy preference. The NITI Aayog principles, however meritorious, do not satisfy this threshold requirement.

**B. The Statutory Framework and Its Deficiencies:** The Information Technology Act, 2000 — designed for electronic commerce and cybercrime — contains no definition of AI, no obligations calibrated to algorithmic decision-making, and no institutional architecture for AI supervision.[17] The Digital Personal Data Protection Act, 2023, while establishing a data protection foundation, does not constitute an AI governance framework: it does not require algorithmic impact assessment or explainability; it contains broad governmental exemptions;[18] and it does not address AI systems operating on non-personal or inferentially derived data. The IT Intermediary Guidelines Rules, 2021 impose content moderation obligations on platforms but raise their own constitutional concerns,[19] as illustrated by the Bombay High Court's interim order in Kunal Kamra v. Union of India (2023).[20] Sectoral regulation by SEBI[21] and the RBI addresses domain-specific concerns without cross-sectoral constitutional coherence.

The MeitY advisory of March 2024, which contemplated governmental approval of "under-tested or unreliable" AI models, exemplified the constitutional fragility of executive-led AI governance: issued without clear statutory foundation, subsequently diluted following industry protest, and of uncertain legal enforceability.[22] The episode illustrates a broader pattern: the Indian State seeks to regulate AI through executive instruments that lack the democratic legitimacy, substantive clarity, and constitutional durability that legislation provides.

**Constitutional Analysis**

**A. Article 14: Algorithmic Classification and Non-Arbitrariness:** Article 14 generates two doctrinal streams of direct relevance. The classification doctrine, established through Anwar Ali Sarkar (1952)[23] and elaborated in Ram Krishna Dalmia (1958),[24] requires that state classifications be founded on an intelligible differentia with a rational nexus to the legitimate object of the measure. Algorithmic classifications — generated through statistical inference from training data — may satisfy the formal requirement of intelligible differentia while failing the rational nexus test. A credit-scoring algorithm that classifies individuals by residential postal code employs an identifiable criterion, but the nexus between postal code and creditworthiness may be mediated by constitutionally impermissible factors — caste, religion, socio-economic status — rather than by factors rationally related to the lending decision. Barocas and Selbst have identified five mechanisms through which facially neutral algorithms produce discriminatory

outcomes.[25]

The non-arbitrariness doctrine, articulated in E.P. Royappa v. State of Tamil Nadu (1974) — "equality and arbitrariness are sworn enemies"[26] — is directly engaged by algorithmic opacity. An AI system that generates a consequential determination through inscrutable computational processes, incapable of explanation to the affected individual or a reviewing court, is arbitrary in the constitutional sense regardless of its formal computational structure. The emerging indirect discrimination framework — developed through Navtej Singh Johar (2018)[27] and Lt Col Nitisha (2021)[28] — extends this analysis to AI systems producing systematically discriminatory effects on protected groups, regardless of discriminatory intent.

**B. Article 19: Algorithmic Content Moderation and Democratic Discourse:** Shreya Singhal v. Union of India (2015) established that content-based restrictions on expression must conform to the enumerated grounds of Article 19(2) and avoid impermissible vagueness.[29] Algorithmic content moderation systems deployed at the direction of the State — through the IT Intermediary Rules and MeitY advisories — engage this framework directly. A direction to suppress "false or misleading" information does not correspond to any enumerated ground of Article 19(2). Where such directions are implemented through AI systems whose criteria are vague, evolving, or inscrutable, the Shreya Singhal requirement of determinacy is violated. The challenge extends beyond individual content decisions to algorithmic curation — the systematic shaping of the information environment through recommendation algorithms that determine what citizens see, in what order, and with what prominence. Where state regulation requires or incentivises specific forms of curation, the resulting distortion of democratic discourse engages Article 19(1)(a).

**C. Article 21: Privacy, Surveillance, and the Proportionality Test:** The nine-judge bench in Puttaswamy (2017) recognised three dimensions of privacy — informational, bodily, and decisional — and formulated a four-pronged proportionality test: legitimate aim, suitability, necessity, and balancing.[30] Each prong generates specific requirements for AI deployment. The suitability prong requires empirical evidence of effectiveness — a facial recognition system with documented error rates of up to 34.7% for darker-skinned women[31] fails this requirement for those populations. The necessity prong requires consideration of less restrictive alternatives; deployment of the most privacy-invasive option without such consideration is constitutionally deficient. The balancing prong must account for the structural and chilling effects of pervasive algorithmic surveillance — on political expression, religious practice, and association.

Justice Chandrachud's dissent in Puttaswamy (Aadhaar) (2019) — that "the architecture of Aadhaar creates a centralised database which enables profiling and tracking of individuals"[32] — resonates with accumulating empirical evidence. The research of Dreze, Khera, and colleagues has documented that biometric authentication failures disproportionately affect the elderly, manual labourers, and persons with disabilities,[33] and the CAG's Report No. 24 of 2021 confirmed systemic operational deficiencies.[34] When the denial of food rations through algorithmic failure implicates the right to life — encompassing subsistence as held in Olga Tellis v. Bombay Municipal Corporation (1985) — and when the procedure authorising that denial fails the Maneka Gandhi standard of "fair, just, and reasonable,"[35] the constitutional violation is not merely technical but existential.

**Judicial Role And Institutional Accountability:** Judicial review of algorithmic state action — constitutionally guaranteed under Articles 32 and 226 and identified as a basic structure component in L. Chandra Kumar v. Union of India (1997)[36] — confronts specific institutional challenges. The petitioner must identify a specific decision amenable to challenge, but algorithmic harms are often diffuse and statistical. The respondent authority must explain the basis of the determination, but the opacity of AI systems may render explanation infeasible. The court must evaluate the challenged action against constitutional standards, but the technical complexity of algorithmic systems may exceed judicial competence without specialised assistance.

These challenges do not render judicial review unavailable — the jurisdiction is constitutionally inviolable — but they diminish its practical efficacy. The public interest litigation jurisdiction, expanded through S.P. Gupta v. Union of India (1982),[37] provides a partial accommodation by permitting challenges on behalf of affected populations. The comparative experience is instructive: in State of Wisconsin v. Eric Loomis (2016), the Wisconsin Supreme Court upheld algorithmic sentencing subject to cautionary requirements;[38] in R (Bridges) v. Chief Constable of South Wales Police (2020), the UK Court of Appeal invalidated police facial recognition for inadequate safeguards.[39] The Bridges approach — requiring specific statutory framework, demonstrated suitability, and adequate oversight — aligns more closely with the Indian proportionality framework and should inform Indian judicial engagement with AI challenges. Institutional adaptation is required. Specialised AI benches within the High Courts, supported by court-appointed technical assessors, would enhance judicial capacity without compromising constitutional jurisdiction. The Anuradha Bhasin (2020) decision — extending the proportionality framework to population-level measures[40] — provides the doctrinal foundation for judicial review of population-level algorithmic systems, though the evidentiary framework requires further development.

**Comparative Analysis**

**A. The European Union:** The EU AI Act (Regulation 2024/1689) establishes a comprehensive, risk-based regulatory architecture comprising four tiers: prohibited practices

(social scoring, untargeted biometric scraping, real-time remote biometric identification in public spaces),[41] high-risk systems (subject to ex ante obligations concerning risk management, data governance, transparency, and human oversight), limited-risk systems (specific transparency obligations), and minimal-risk systems (unregulated).[42] The Act's enforcement regime includes penalties of up to •35 million or 7% of global turnover.[43] Its constitutional grounding in the EU Charter of Fundamental Rights demonstrates the feasibility of rights-based AI regulation at scale. India need not adopt the EU architecture wholesale, but the EU's demonstration that categorical prohibitions, mandatory impact assessments, and institutional oversight are operationally achievable is analytically significant.

**B. The United States:** The US approach has been characterised by executive volatility — Executive Order 14110 (October 2023) established comprehensive AI safety requirements, only to be revoked by Executive Order 14179 (January 2025).[44] State-level legislation, particularly the Colorado AI Act (2024),[45] and sectoral enforcement by the FTC, EEOC, and CFPB provide partial coverage but generate fragmentation. The US experience is instructive primarily in its limitations: reliance on executive action produces regulatory instability; the sectoral approach leaves systemic gaps; and the absence of a comprehensive constitutional framework analogous to Part III reduces the normative resources available for judicial engagement.

**C. Lessons for India:** The comparative analysis supports three propositions. First, legislative rather than executive foundations are constitutionally necessary for AI governance — a requirement derived from the rule of law principle and reinforced by the US experience of executive volatility. Second, risk-based regulatory architecture — calibrating the stringency of obligations to the constitutional severity of the deployment — provides a proportionate framework consistent with Article 14's requirement of reasonable classification. Third, institutional independence of the regulatory authority — insulating AI oversight from the executive's dual role as promoter and regulator — is constitutionally essential for credible accountability. Kaminski's analysis of the GDPR's approach to algorithmic accountability confirms that individual rights-based and systemic oversight-based mechanisms must be integrated rather than treated as alternatives.[46]

**Key Challenges:** Four structural challenges impede constitutional accountability for AI in India. First, **algorithmic opacity**: the inscrutability of AI decision processes defeats the constitutional requirement of reasoned state action. The convergence of Article 14 non-arbitrariness, Article 21 procedural fairness, and the requirement of reasoned orders implies a constitutional right to explanation for consequential algorithmic decisions — a right not textually enumerated but implicit in established doctrine. Second, **diffused liability**: when AI systems are designed by private firms, trained on third-party data, procured by government agencies, and deployed by institutional operators, the identification of the constitutionally responsible actor becomes structurally problematic. Third, the **absence of an enforceable regulatory framework**: the current patchwork of general-purpose statutes, subordinate rules, and non-binding policy documents leaves categories of AI-related conduct that engage fundamental rights outside the regulatory scope of any existing instrument. Fourth, the **risk of executive overreach**: the MeitY advisory episode of March 2024 demonstrated that executive instruments may be deployed to regulate AI — including through prior-approval requirements — without the constitutional safeguards that parliamentary legislation provides.

**Normative Recommendations:** The foregoing analysis supports five constitutionally grounded reforms. First, Parliament should enact a **comprehensive Artificial Intelligence Act** establishing a risk-based regulatory architecture with four tiers (prohibited, high-risk, limited-risk, minimal-risk), mandatory obligations calibrated to the constitutional risk of each tier, and rights and remedies for affected individuals. The Act must preserve judicial review under Articles 32 and 226, consistent with L. Chandra Kumar.[47]

Second, the Act should mandate **algorithmic impact assessments** before the deployment of high-risk AI systems by public authorities — operationalising the Puttaswamy proportionality test ex ante rather than relying exclusively on post-deployment judicial review. The assessment should include disaggregated accuracy analysis, identification of less restrictive alternatives, and plans for ongoing monitoring.

Third, the Act should establish **statutory explainability obligations** — creating a right to be informed of AI involvement in a consequential determination, to receive a meaningful explanation, and to obtain human review. This statutory right operationalises the constitutional right to explanation that emerges from the convergence of Articles 14 and 21.

Fourth, Parliament should establish an **independent AI Regulatory Authority of India** with cross-sectoral jurisdiction, modelled on existing independent regulators (SEBI, CCI, TRAI). The Authority's functions should include registration of high-risk systems, review of impact assessments, algorithmic auditing, complaint investigation, and coordination with sectoral regulators.

Fifth, the courts should develop **constitutional tort remedies** for AI-generated harm through the extension of the Nilabati Behera[48]/D.K. Basu[49] doctrine. A statutory presumption of state liability for consequential AI deployments — with the deploying authority entitled to seek contribution from private contractors — would preserve constitutional accountability while addressing the attribution difficulties inherent in algorithmic harm. The European Commission's proposed AI Liability Directive, introducing a rebuttable presumption of causation,[50] provides a

comparative model for adaptation within the Indian constitutional tradition.

**Conclusion:** The Constitution of India, as Granville Austin observed, is "first and foremost a social document"[51] — a document whose protections must be rendered operationally effective against every form of consequential power, including algorithmic power. This paper has argued that the established constitutional framework — the non-arbitrariness doctrine of Royappa, the due process framework of Maneka Gandhi, the privacy architecture and proportionality test of Puttaswamy, the content-regulation standard of Shreya Singhal, and the basic structure doctrine of Kesavananda Bharati[52] — provides a substantially adequate normative framework for disciplining AI-mediated state action. What is absent is not constitutional doctrine but the statutory, institutional, and operational architecture necessary to translate that doctrine into governance.

The trajectory of AI constitutionalism in India will depend on whether the institutions of the Republic — the Legislature, the Executive, and the Judiciary — summon the commitment necessary to close this gap. The legislative enactment of a comprehensive AI statute, the judicial recognition of a constitutional right to explanation, the establishment of an independent regulatory authority, and the development of constitutional tort remedies for algorithmic harm are each constitutionally required steps. Each is operationally feasible, as comparative experience demonstrates. And each is constitutionally urgent, because the deployment of AI in Indian governance is not a future prospect but a present reality — a reality in which the fundamental rights of hundreds of millions of citizens are engaged by algorithmic systems that the existing regulatory framework is structurally inadequate to govern.

The question is not whether the Constitution can discipline algorithmic power. It can. The question is whether it will be permitted to do so.

**References:-**

1. NITI Aayog, National Strategy for Artificial Intelligence #AIForAll, Discussion Paper, Government of India, New Delhi, June 2018, at 13-17.
2. NCRB, Request for Proposal for National Automated Facial Recognition System (AFRS) (June 28, 2019).
3. Internet Freedom Foundation, Project Panoptic: Database of FRT Deployments in India (2022).
4. India Const. art. 14.
5. India Const. art. 19(1)(a).
6. India Const. art. 21.
7. Regulation (EU) 2024/1689, of the European Parliament and of the Council of 13 June 2024, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).
8. Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 3 (2015).
9. Mireille Hildebrandt, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology 171-84 (2015).
10. Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1270-1300 (2008).
11. Jack M. Balkin, The Three Laws of Robotics in the Age of Big Data, 78 Ohio St. L.J. 1217, 1230-36 (2017).
13. NITI Aayog, Responsible AI for All: Approach Document for India - Part 1, Government of India, Feb. 2021, at 12-18.
14. Ministry of Electronics and Information Technology, Report of the Sub-Committee on AI Governance and Guidelines Development, Government of India, 2024, at 8-14.
15. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301, paras 18-19 (India).
16. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, para 325 (India).
17. Information Technology Act, 2000, No. 21 of 2000, India Code (as amended 2008).
18. Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code, secs. 17(2)-(3).
19. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, GSR 139(E), as amended.
20. Kunal Kamra v. Union of India, (2023) 4 Bom CR 475 (India).
21. SEBI, Circular on Use of AI and ML by Market Intermediaries, SEBI/HO/MIRSD/DOS2/CIR/P/2019/10 (Jan. 4, 2019).
22. MeitY, Advisory on Due Diligence by Intermediaries, No. 2(4)/2023-CyberLaws-3 (Mar. 1, 2024), as modified (Mar. 15, 2024).
23. State of West Bengal v. Anwar Ali Sarkar, AIR 1952 SC 75, paras 12-16 (India).
24. Ram Krishna Dalmia v. S.R. Tendolkar, AIR 1958 SC 538, paras 11-13 (India).
25. Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Calif. L. Rev. 671, 677-93 (2016).
26. E.P. Royappa v. State of Tamil Nadu, AIR 1974 SC 555, para 85 (India).
27. Navtej Singh Johar v. Union of India, (2018) 10 SCC 1, paras 241-60 (India).
28. Lt Col Nitisha v. Union of India, (2021) 15 SCC 125, paras 62-65 (India).
29. Shreya Singhal v. Union of India, (2015) 5 SCC 1, paras 76-89 (India).
31. Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proc. Mach. Learning Res. 1 (2018).
32. Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2019) 1 SCC 1, paras 447-49 (Chandrachud, J., dissenting) (India).
33. Jean Dreze, Nazar Khalid, Reetika Khera & Anmol Somanchi, Aadhaar and Food Security in Jharkhand:

Pain without Gain?, 52(50) Econ. & Pol. Wkly. 50 (2017).
34. CAG, Report No. 24 of 2021 on Functioning of UIDAI, paras 4.1-4.15.
35. Maneka Gandhi v. Union of India, AIR 1978 SC 597, para 7 (India).
36. L. Chandra Kumar v. Union of India, (1997) 3 SCC 261, para 78 (India).
37. S.P. Gupta v. Union of India, AIR 1982 SC 149 (India).
38. State of Wisconsin v. Eric Loomis, 881 N.W.2d 749 (Wis. 2016).
39. R (Bridges) v. Chief Constable of South Wales Police [2020] EWCA Civ 1058 (U.K.).
40. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637, paras 152-64 (India).
41. Id. art. 5 (prohibited AI practices).
42. Regulation (EU) 2024/1689, supra note 2, arts. 5-6, 9-15, 50-56.
43. Id. arts. 99-101 (penalties up to EUR 35 million or 7% of global annual turnover).
44. Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Nov. 1, 2023), revoked by Exec. Order No. 14,179, 90 Fed. Reg. 8,741 (Jan. 31, 2025).
45. Colorado AI Act, SB24-205, Colo. Rev. Stat. secs. 6-1-1701 to 6-1-1707 (2024).
46. Margot E. Kaminski, Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability, 92 S. Cal. L. Rev. 1529, 1540-55 (2019).
48. Nilabati Behera v. State of Orissa, (1993) 2 SCC 746, paras 16-17 (India).
49. D.K. Basu v. State of West Bengal, (1997) 1 SCC 416, paras 54-55 (India).
50. European Commission, Proposal for a Directive on AI Liability, COM(2022) 496 final (Sept. 28, 2022).
51. Granville Austin, The Indian Constitution: Cornerstone of a Nation 50 (1966).
52. Kesavananda Bharati v. State of Kerala, AIR 1973 SC 1461, para 316 (India).

**********