CANONSPHERE
LAW REVIEW

ISSN: 3107-460X (Online)

CANONSPHERE LAW REVIEW

Volume 1 Issue 3

July to September, 2025

TABLE OF CONTENTS

Algorithmic Accountability and the Law in India: Governing AI in Autonomous and Critical Sectors

This long article is written by SUMITHRA S, co authored by RUTHRA B

Abstract: The governance of AI systems used in independent and vital industries like healthcare, finance, defense, and public administration is the main focus of this paper which examines the boundaries of algorithmic accountability in India. It looks at the doctrinal, ethical, and legal aspects of accountability, placing AI governance within industry-specific regulatory frameworks, emerging jurisprudence, and constitutional principles. The study examines the effectiveness of legislative measures, court rulings, and policy directives in mitigating the risks associated with multi-stakeholder AI ecosystems and opaque decision-making processes. It also explores explainability, transparency, algorithmic audits, and liability distribution among developers, operators, and end users, emphasising the practical and normative requirements for responsible AI deployment. In order to propose a comprehensive governance model, the paper makes policy recommendations that include algorithmic impact assessments, adaptive compliance frameworks, and the integration of ethical and human rights protections. This study adds to the continuing conversation on AI accountability in India by combining legal theory, regulatory practice, and interdisciplinary insights, providing workable frameworks to balance technological advancement with social protection.

Keywords: Algorithmic Accountability, AI Governance, Autonomous Systems, Liability, Transparency, Explainable AI, Indian Legal Framework, Critical Sectors, Policy Recommendations, Ethical Oversight.

INTRODUCTION

The decision in ***Justice K.S. Puttaswamy v. Union of India,*** states that "the pursuit of technology cannot become an alibi to deny citizens their dignity." This statement assumes new meaning in the era of artificial intelligence (AI), when technological developments quickly intersect with constitutional rights and governance. Once viewed as a distant possibility, artificial intelligence (AI) is now widely employed in India's financial, medical, military, and public administration sectors. While its integration promises transformative benefits, it also raises systemic issues like algorithmic bias, opacity, and challenges with accountable decision-making. As scholars like Frank Pasquale and Danielle Citron have noted, algorithms often function as "black boxes," avoiding transparency and undermining basic ideas of justice and due process. This opacity poses a serious threat to the traditional theories of culpability and accountability, which form the basis of constitutional democracies such as India. Unlike the European Union, which has implemented comprehensive, risk-based frameworks for reliable AI, India's regulatory environment is still fragmented, with sector-specific guidelines, draft data protection legislation, and occasional judicial interventions. This fragmentation makes it harder to place blame when autonomous systems fail or produce discriminating outcomes. In intricate multi-stakeholder ecosystems involving developers, operators, and end users, where doctrinal clarity is still lacking, defining culpability becomes particularly challenging.

In this sense, algorithmic responsibility in India should not be seen as merely a technical problem but rather as a moral obligation. Legal frameworks must both promote innovation and guard against its excesses in order to guarantee that technological advancement upholds democratic values rather than technocratic ones. Explainability, transparency, and algorithmic auditing must be institutionalised through the use of frameworks based on strict responsibility, negligence, and constitutional torts. Beyond legal issues, ethical principles like justice, human dignity, and inclusivity should direct the use of AI in critical industries.

A major scholarly gap is filled in this study. The doctrinal underpinnings of liability and accountability in AI governance have received little attention, despite the fact that privacy and data protection have dominated Indian conversation. This analysis suggests conceptual pathways that are specific to India's constitutional framework by placing Indian discussions within global regulatory tendencies. As a result, it analyses statute provisions, policy implementation, and judicial activism to investigate the doctrinal, regulatory, and ethical aspects of algorithmic responsibility. The inquiry is structured around two central research questions:(i) How can Constitutional principles of equality, dignity, and due process inform the governance of Algorithmic decision-making in India?

(ii) Which doctrinal and regulatory frameworks are most suitable for allocating responsibility across multi-stakeholder AI ecosystems?

CONCEPTUAL FOUNDATIONS OF ALGORITHMIC ACCOUNTABILITY

Aadhaar authentication failures in 2019 affected over 8 million citizens, as reported. This was a tangible manifestation of the worldly impact of errors in algorithmic systems governing access to critical services. Since artificial intelligence continues to inform important decisions in India - ranging from machine learning-based credit scores in fintech to AI-based diagnostics in healthcare and defence decision-support systems - accountability has become an urgent legal, moral, and social necessity. These system failures or biases are not just technical problems; they carry deep implications for due process, dignity, and equality. Algorithmic accountability addresses how institutions, operators, and developers can be held accountable for decisions informed by or generated through AI systems. This creates a multifaceted framework at the intersection of technology, law, ethics, and governance. Conventional concepts of responsibility, based on the direct human input, differ from algorithmic accountability. Distributed agency, including code, data sets, system design, and deployment context, determines the output of AI systems. Scholars like Frank Pasquale and Danielle Citron identify the "black box" phenomenon of modern AI. This contradicts classical legal notions of responsibility and serves as a sign of growing need for explicitly formulated regulatory models, normative theory, and firm legal doctrine.[1]

Drawing from such theoretical concepts, India's judiciary has to look at constitutional safeguards. Public and private stakeholders must abide by the equality rights under **Article 14,** right to life and liberty under **Article 21**, and privacy as interpreted in the case ***Justice K.S. Puttaswamy v. Union of India***.[2] They must also ensure that AI systems do not debase human dignity, discriminate, or function in a way that undermines due process. Indian law such as the, Reserve Bank of India Guidelines on Artificial Intelligence in Financial Services, and defense and healthcare-specific legislation complements such safeguards by establishing accountability throughout the life cycle of AI systems.

Some real-world impacts include Aadhaar authentication issues impacting the rights of citizens, discriminatory automatic credit scoring algorithms used in fintech, and AI-augmented diagnosis errors in public hospitals. Algorithmic ecosystems tend to have a variety of stakeholders, including operators, developers, producers of data, and end users. For successful accountability, frameworks need to define responsibilities at every step, from design through implementation and operational observation[3].

International regulatory models like the European Union's Artificial Intelligence Act, the Organisation for Economic Co - operation and Development principles on Artificial Intelligence, and Singapore's Model AI Governance Framework stress risk-based responsibility, transparency, explainability, and auditability. These models are instructive, but for India, take into consideration that they need to account for differences in regulatory systems, judicial responses, socioeconomic diversity, and industry-specific concerns. Algorithmic responsibility in India is based on four interconnected pillars. Transparency ensures stakeholders to be able to understand the databases, parameters, and rules behind automated decision-making. Outcomes must be understandable and contextually based to be explainable[4].

Auditability entails establishing independent and ongoing monitoring procedures that are capable of identifying errors, bias, or malpractice. Lastly, allocation of liability decides lawful and ethical responsibilities of all parties in the AI ecosystem. By placing algorithmic responsibility within constitutional provisions, open legal principles, and ethical norms, India can build a system balancing technological innovation and societal protection. This approach gives the country a basis to quantify the governance of AI systems in autonomous and critical sectors so that the country can leverage AI as an instrument of just, equitable, and accountable governance.[5]

AUTONOMOUS SYSTEMS IN CRITICAL SECTORS: LEGAL AND SOCIETAL STAKES

The deployment of autonomous systems in critical sectors - healthcare, finance, defense, and public administration - raises profound legal and societal questions that transcend technical considerations. These systems, designed to operate with minimal human intervention, promise efficiency, predictive accuracy, and cost savings. Yet, their autonomy amplifies risks of error, bias, and opacity, creating accountability gaps with direct consequences for constitutional rights and public trust.

Healthcare: AI-assisted diagnostic tools and autonomous surgical systems are increasingly piloted in Indian hospitals to address resource shortages and improve efficiency.[6] These technologies enhance diagnostic accuracy and reduce human error, yet flawed training data or biased models have already resulted in misdiagnoses, exposing patients to life-threatening risks. Without sector-specific liability rules, courts must grapple with whether responsibility lies with manufacturers, software developers, or healthcare institutions. Such failures implicate the constitutional right to life and health under Article 21,[7] where negligence and strict liability doctrines may provide a partial but inadequate framework for accountability.

Finance: Autonomous credit-scoring and fraud-detection models dominate India's fintech ecosystem, enabling rapid financial inclusion but also embedding systemic bias.[8] Marginalized groups, particularly those lacking robust credit histories, face discriminatory outcomes driven by skewed datasets and opaque architectures. Such practices directly implicate Article 14's equality mandate and have invited judicial scrutiny under the doctrine of arbitrariness.[9] While the Reserve Bank of India has issued preliminary guidelines,[10] doctrinal clarity on liability remains elusive, particularly when harm stems from systemic design flaws rather than identifiable misconduct by an operator.

Defense: The most ethically fraught domain is defense, where autonomous weapons and AI-driven decision-support systems are under trial.[11] Though their deployment promises strategic advantages, they heighten risks of civilian harm, ethical violations, and breaches of international humanitarian law. India's constitutional commitment to dignity and proportionality,[12] coupled with its obligations under international law, demands doctrinal clarity before such systems are integrated into live operations. Absent clear accountability, military autonomy risks undermining both democratic oversight and humanitarian norms.

Public Administration: The use of autonomous tools in welfare distribution and predictive policing illustrates the tension between efficiency and rights protection. Based on aadhar authentication errors have excluded millions from essential entitlements, undermining socio-economic rights, structural gaps in administrative accountability.[13] Inequalities raising constitutional concerns under Articles 14 and 21.[14] In both contexts, the lack of independent audits and transparent oversight mechanisms deepens the democratic deficit.

From a societal perspective, integrating autonomous systems into these critical domains risks eroding public trust unless robust accountability mechanisms are institutionalized. Indian law must therefore evolve to provide clear liability allocation, mandate algorithmic audits, and preserve human oversight in high-stakes decisions. Comparative models such as the European Union's AI Act, which designates "high-risk" sectors for stricter obligations, provide valuable guidance but must be adapted to India's fragmented regulatory environment and socio-economic diversity.[15]

Therefore, the legal and societal stakes of autonomous systems lie in reconciling technological innovation with the imperatives of constitutionalism, rights protection, and democratic governance. Without a coherent accountability framework, the very efficiency gains promised by autonomy risk being overshadowed by systemic injustices, arbitrary exclusions, and erosion of fundamental rights.

THE BLACK BOX MEETS THE CONSTITUTION: CHARTING INDIA'S AI GOVERNANCE DEFICITS

The metaphor of the "black box" aptly captures the opacity and inscrutability of contemporary AI systems, where the decision-making logic remains concealed even from their own designers. In India, this opacity intersects with the constitutional promise of equality, dignity, and due process, creating profound governance deficits. Algorithmic decision-making now mediates access to healthcare, credit, welfare, and even defense, yet its opacity resists accountability, undermining constitutional safeguards that require state and private action to remain transparent, proportionate, and justifiable.[16]

Unlike the European Union's Artificial Intelligence Act, which adopts a risk-tiered and ex ante regulatory architecture,[17] India lacks a consolidated statutory regime for AI. First, the allocation of liability within multi-stakeholder AI ecosystems remains indeterminate. Developers, data providers, operators, and state institutions share overlapping roles, but no clear doctrine specifies responsibility when autonomous systems malfunction or perpetuate bias. Traditional negligence or strict liability doctrines prove inadequate when harms result from diffuse algorithmic processes rather than discrete human action. Without doctrinal innovation - possibly through constitutional torts—victims of algorithmic harm face formidable barriers to redress.

Second, India's regulatory silence on algorithmic transparency exacerbates constitutional risks. Articles 14 and 21 demand that state action be non-arbitrary and rights-respecting, yet welfare exclusions from Aadhaar authentication failures and discriminatory outcomes in fintech credit-scoring illustrate the constitutional consequences of black-box governance.

Courts have occasionally intervened, invoking arbitrariness and proportionality, but in the absence of systematic audit frameworks, judicial review remains reactive and fragmented.

Global models underscore what India lacks. The EU mandates algorithmic impact assessments and imposes heightened obligations on “high-risk” systems, while Singapore’s Model AI Governance Framework operationalizes principles of explainability and accountability. India’s reliance on soft law - policy papers, committee reports, and sectoral circulars does little to institutionalize these safeguards.

DOCTRINAL PRINCIPLES INFORMING AI LIABILITY IN INDIAN LAW

In critical sectors exposes a doctrinal lacuna intersect with Indian law. Classical legal frameworks—such as negligence, strict liability, and vicarious liability—were designed for discrete human action and are inherently ill-suited for algorithmic harm, which arises from distributed agency encompassing developers, data architects, operators, and institutional oversees[18] . AI systems, often operating as “black boxes,” challenge the foundational assumption of direct human control over outcomes. Consequently, doctrinal innovation is necessary to reconcile liability with constitutional mandates, including the rights to equality (Article 14), life and personal liberty (Article 21), and dignity.[19]

1. Expanding Negligence and Duty of Care: Negligence in Indian law traditionally requires the existence of a duty, breach, causation, and damage. In AI contexts, courts must extend the duty of care to encompass developers, operators, and data providers whose actions - or omissions - in model design, training, and deployment foreseeable create harm[20] .For instance, biased automated credit scoring or flawed AI-assisted diagnostics demonstrates that negligence cannot be confined to end-user actions; liability must capture systemic design flaws and foreseeability in multi-stakeholder ecosystems. Judicial precedents such as ***Indian Medical Association v. Union of India*** highlight the duty of public authorities to exercise care in delivering essential services, which can analogically support AI liability in healthcare and public administration.[21]

2. No-Fault Liability: Strict liability doctrines, historically applied to hazardous industrial activity ***(Rylands v. Fletcher) and further elaborated in M.C. Mehta v. Union of India,*** offer a compelling model for AI.[22] Autonomous systems in healthcare, defense, and fintech generate risks that are inherently difficult to predict or control, warranting a no-fault liability regime for operators and developers. By imposing responsibility irrespective of intent or negligence, such doctrines incentivize robust safety measures, regular audits, and algorithmic transparency, aligning accountability with the constitutional imperative of non-arbitrariness under Articles 14 and 21.[23]

3. Constitutional Torts and Public Law Liability: Where AI is deployed by state actors, classical torts may prove inadequate. Constitutional torts provide a mechanism to redress rights violations arising from algorithmic governance. For example, welfare exclusion due to Aadhaar authentication failures implicates Articles 14 and 21, enabling judicial intervention even in the absence of explicit statutory remedies ***(Ram Jethmalani v. Union of India)***.[24] Similarly, principles from ***Anuradha Bhasin v. Union of India*** and ***E.P. Royappa v. State of Tamil Nadu*** underscore procedural fairness, proportionality, and anti-arbitrariness, which must inform the deployment of AI systems that mediate access to essential services.[25]

4. Hybrid Doctrinal Innovation: Effective AI accountability in India requires a hybrid doctrinal model, integrating:

a. Expanded negligence capturing multi-stakeholder responsibility.

b. Strict liability for inherently high-risk AI systems.

c. Constitutional tort principles for state-led algorithmic interventions.

This framework simultaneously fosters technological innovation and enforces accountability, ensuring that autonomous systems advance social welfare while remaining aligned with constitutional norms. Comparative insights from Singapore's Model AI Governance Framework and the EU AI Act reinforce the need for risk-based, proportionate, and transparent regulatory measures, which Indian law must adapt contextually to socio-economic diversity, fragmented regulatory structures, and judicial activism[26]. In sum, doctrinal principles for AI liability in India cannot remain static. They must evolve to bridge technological complexity and legal accountability, providing actionable remedies that respect rights, incentivize ethical AI design, and preserve public trust in autonomous governance. By fusing tort law, constitutional imperatives, and comparative regulatory strategies, India can cultivate a rights-respecting, innovation-friendly liability framework suitable for the AI-driven era.

FROM OPACITY TO OVERSIGHT: TRANSPARENCY, EXPLAINABILITY, AND ALGORITHMIC AUDITS

Artificial intelligence systems have long been criticized for their opacity, often described as "black boxes" where decisions are made in ways that are difficult to trace or understand. This lack of clarity raises concerns about accountability, bias, and fairness, particularly when AI is deployed in sensitive sectors as criminal justice, healthcare, and finance. Deliberate design and regulatory approaches are necessary to go from opacity to oversight, making AI systems socially responsible in addition to technically dependable. Both developers and end users can examine and have faith in algorithmic processes thanks to the two pillars of transparency and explainability that support this shift.

Transparency prioritises organised disclosure on several levels, including recording development iterations, publishing and documenting data sources, and ensuring stakeholders can see governance procedures. Clarity on what influences AI judgements can be achieved, for instance, by labelling synthetic data, keeping datasets with transparent version histories, and revealing. third-party integrations via a software bill of materials **("SBOM")**. Operationally speaking, transparency also entails stating who is in charge of supervision, the purpose of each system, and the procedures for handling mistakes or abuse. This embeds accountability within governance frameworks and makes it possible for external audits, compliance checks, and stakeholder communication in ways that go beyond simple technical reporting.

However, the need for explainability in AI is not only a matter of taste; it is also a moral requirement. Decisions pertaining to employment, justice, health, and financial stability are increasingly influenced by AI systems, therefore stakeholders need to be able to understand, analyse, and question algorithmic outcomes. Mittelstadt (2021) emphasizes that opaque AI systems undermine moral agency by stripping individuals of the ability to understand or appeal outcomes that significantly shape their lives. From a consequentialist standpoint, explainability minimizes harm and maximizes benefits by enabling bias detection, error correction, and accountability through human oversight[27]. Arrieta et al. (2020) further note that interpretability acts as a safeguard, ensuring that human intervention remains possible in the case of wrongdoing or system failure.[28]

Transparency and explainability also intersect with concepts of procedural justice and democratic accountability. A lack of clarity in algorithmic processes undermines public trust, particularly in high-stakes applications like law enforcement or public administration. Rudin (2021) argues that the reliance on black-box models in such contexts is ethically indefensible when interpretable alternatives exist. In healthcare, explainability is tied directly to autonomy and informed consent, as patients must understand diagnoses and treatment options.[29] Manche and Myakala (2022) emphasize that explainability is critical not only for debugging large language models but also for aligning them with patient-centered care and the principles of informed consent.[30] Importantly, what counts as a "sufficient explanation" may vary across cultural, legal, and institutional contexts, requiring a contextual and stakeholder-sensitive approach.

Taken together, transparency and explainability are not simply tools of technical oversight but mechanisms of ethical governance. They bridge normative values with practical safeguards, ensuring that algorithms are not left as unchallengeable authorities but as accountable, auditable systems aligned with human dignity and justice. Achieving this requires interdisciplinary strategies that embed transparency in data and governance, foster explainability through human-readable reasoning, and adapt frameworks to diverse social contexts.

ALLOCATING RESPONSIBILITY IN COMPLEX AI ECOSYSTEMS: ANALYSING THE MULTI-STAKEHOLDER CHALLENGE

In complex multi-stakeholder ecosystems that include developers, vendors, regulators, operators, and end users, artificial intelligence (AI) systems operate. The spread of agency and this diffusion of agency complicates the attribution of liability, as harms rarely originate from a single actor but from the interaction of multiple roles. Traditional doctrines such as negligence, strict and absolute liability, and constitutional torts were built upon linear causation models, yet AI systems operate through recursive feedback loops, where outcomes are shaped by data, deployment contexts, and adaptive learning.[31] The result is an accountability puzzle: who bears responsibility when algorithmic decisions infringe rights or cause harm? The classical maxim *ubi jus ibi remedium* reminds us that where there is a right, there must be a remedy, yet in India's current regime, victims of algorithmic harm often confront a remedial vacuum.

Comparative experience highlights potential pathways. The European Union's AI Act (2024) establishes a risk-tiered, ex-ante accountability framework, mandating algorithmic impact assessments, conformity obligations, and duties distributed across the AI lifecycle, ensuring that liability does not vanish into the "black box."[32] The United States has relied on FTC enforcement actions and scholarly proposals for adaptive tort doctrines that apportion liability according to actors' ability to mitigate harm.[33] China, by contrast, adopts a command-and-control approach, with its 2022 Algorithmic Regulation Rules directly obligating providers to prevent discrimination and ensure transparency.[34] India, however, remains tethered to fragmented frameworks: the Information Technology Act, 2000, sectoral rules, and non-binding policy documents such as NITI Aayog's Responsible AI for All (2021), which outlines fairness and inclusivity principles without enforceable liability structures.[35]

Indian jurisprudence provides constitutional footholds for reform. In ***Justice K.S. Puttaswamy v. Union of India,*** the Supreme Court underscored that technological innovation cannot override dignity and privacy, setting normative limits on automated governance. In Shreya Singhal v. Union of India, the Court stressed precision and proportionality in technology regulation, reinforcing the need for clarity in assigning responsibility.[36] In ***Nilabati Behera v. State of Orissa,*** the doctrine of constitutional torts was advanced to ensure compensation for violation of fundamental rights, demonstrating judicial willingness to impose strict state liability.[37] Likewise, in ***M.C. Mehta v. Union of India,*** the Court's articulation of absolute liability for hazardous activities offers a doctrinal template for AI, which, though intangible, produces systemic risks comparable in magnitude.[38] These principles indicate that Indian courts already possess a constitutional vocabulary to extend liability doctrines into AI governance.

At a normative level, scholars like Andreas Matthias have identified an "accountability gap," arguing that autonomous systems cannot themselves bear responsibility, leaving liability to be anchored in human agency.[39] Luciano Floridi and others emphasise embedding fairness, transparency, and explainability as governance imperatives. This aligns with constitutional values under Articles 14 and 21, ensuring that AI-driven decision-making respects equality, dignity, and due process.[40] To reconcile these demands, India must move towards a layered accountability model - one that distributes liability proportionately among stakeholders based on their role and capacity to prevent harm, mandates algorithmic audits and impact assessments, and anchors oversight within constitutional safeguards.

Ultimately, allocating responsibility in complex AI ecosystems is not merely a technical challenge but a constitutional and normative imperative. The Latin maxims *fiat justitia ruat* *caelum* (“let justice be done though the heavens fall”) and *salus populi suprema lex* (“the welfare of the people is the supreme law”) underscore the need for legal regimes that prioritise justice and collective welfare, even amid technological opacity.

VIII. Policy and Regulatory Recommendations for Robust AI Governance in India

The AI Governance Framework for India 2025–26, developed by the National Cyber and AI Centre **(“NCAIC”)**, advances a set of policy and regulatory measures designed to embed trust, accountability, and resilience into India’s AI ecosystem. At its foundation, the framework emphasizes human-centricity, inclusivity, and proportionality of risk, aligning AI deployment with constitutional values and global best practices (NCAIC, 2025).

First, the framework recommends regulatory harmonization across India’s existing legal instruments. It explicitly aligns AI governance with the Digital Personal Data Protection Act **(“DPDP”)**, CERT-In directives, sectoral laws, and the India AI Mission, ensuring consistency between AI oversight and the broader digital governance ecosystem (NCAIC, 2025). To operationalize this, it proposes a multi-tier governance model, introducing AI Risk and Ethics Committees **(“AIREC”)** at institutional levels and designating Chief AI Risk Officers **(“CAROs”)** to oversee compliance, risk mitigation, and reporting. Secondly, it provides taxonomy used cases. The controls are recommend for AI system, data governance, secure development, monitoring and decommissioning protocols. Thirdly, introduces tiered assurance and certification, offering basic and premium certification by individual audits for example mandating transparency. Finally, it framework international alignment and cultural adaptability. At the same time, it acknowledges domestic needs such as digital inclusion, and sustainability as guiding principles for responsible deployment (NCAIC, 2025).

CONCLUSION

Regulation of AI in India's critical and autonomous sectors now presents enormous opportunities as well as urgent risks. Algorithmic accountability is a constitutional, legal, and ethical requirement that should not be solely considered from a technical standpoint. The current patchwork of regulations in India, which includes frameworks specific to different sectors, consumer law, financial regulation, and data protection, underscores the need for a more unified, principle-based model that supports liability, explainability, and transparency while facilitating technological advancement. To do this, developers, regulators, businesses, and users must all share responsibility in addition to adhering to the law. While tort law doctrines, constitutional protections, and statutory obligations adjust to technological realities, it is crucial to ground AI governance in values like justice, autonomy, fairness, and human dignity. At this point, India can stop adopting international models and start establishing responsible AI governance by implementing risk-based regulation, algorithmic audits, and more robust policy integration. In a rapidly evolving digital society, such a framework not only protects citizens but also fosters democratic legitimacy, public trust, and ethical resilience.

REFERENCES

[1] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harv. Univ. Press 2015) (Harv. Univ. Press 2015).

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

[3] Press Information Bureau, Government of India, *Aadhaar Authentication Failure Reports* (2019); Reserve Bank of India, *Automated Credit Risk Reports* (2021); Ministry of Health & Family Welfare, *AI Diagnostic Systems Review* (2022); Ministry of Defence, *Autonomous Systems Trial Report* (2021).

[4] European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence* (AI Act) COM (2021) 206 final; OECD, OECD *Principles on Artificial Intelligence* (2019); Infocomm Media Development Authority of Singapore, *Model AI Governance Framework* (2020).

[5] Information Technology Act, No. 21 of 2000, §§ 43A, 66 (India); Reserve Bank of India, *Guidelines on Use of Artificial Intelligence in Financial Services* (2021); Ministry of Health & Family Welfare, *Clinical Establishments Act Regulations* (India, 2010).

[6] Ministry of Health & Family Welfare, *AI Diagnostic Systems Review* (2022).

[7] INDIA CONST. art. 21; *Paschim Banga Khet Mazdoor Samity v. State of W.B.,* (1996) 4 SCC 37 (India).

[8] Reserve Bank of India, *Automated Credit Risk Reports* (2021).

[9] INDIA CONST. art. 14; E.P. *Royappa v. State of T.N.,* (1974) 4 SCC 3 (India).

[10] Reserve Bank of India, *Guidelines on Use of Artificial Intelligence in Financial Services* (2021).

[11] Ministry of Defence, *Autonomous Systems Trial Report* (2021).

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

[13] Reetika Khera, *Impact of Aadhaar-Linked Welfare Exclusion in India*, 54 Econ. & Pol. Wkly. 50 (2019).

[14] Apar Gupta, *Predictive Policing and Constitutional Rights in India*, Internet Freedom Found. Report (2020).

[15] European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence* (AI Act), COM (2021) 206 final.

[16] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harv. Univ. Press 2015) (Harv. Univ. Press 2015).

[17] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final.

[18] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harv. Univ. Press 2015).

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

[20] Shreya Sinha, *"Algorithmic Liability and Indian Tort Law: Emerging Doctrinal Challenges"* (2022) 5 NUJS L. Rev. 101.

[21] *Indian Medical Association v. Union of India,* (2011) 7 S.C.C. 179.

[22] *Rylands v. Fletcher,* (1868) L.R. 3 H.L. 330 (U.K.); see also *M.C. Mehta v. Union of India,* (1987) 1 S.C.C. 395.

[23] *E.P. Royappa v. State of Tamil Nadu,* (1974) 4 S.C.C. 3; *Anuradha Bhasin v. Union of India,* (2020) 3 S.C.C. 637.

[24] *Ram Jethmalani v. Union of India,* (2011) 4 S.C.C. 1.

[25] Reetika Khera, *"Aadhaar Failures: Rights and Accountability in the Welfare State"* (2019) 54(5) Economic and Political Weekly 12.

[26] INFOCOMM MEDIA DEV. AUTH., *Model AI Governance Framework* (2d ed. 2020) (Sing.); European Commission, Proposal for a Regulation *Laying Down Harmonised Rules on Artificial Intelligence* (Artificial Intelligence Act), COM(2021) 206 final.

[27] B. D. Mittelstadt, *Principles Alone Cannot Guarantee Ethical AI*, 3 Nature Mach. Intell. 783, 783–85 (2021).

[28] B. Arrieta et al., *Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges Toward Responsible AI*, 58 Information Fusion 82, 82–115 (2020).

[29] C. Rudin, *Stop Explaining Black Box Machine Learning Models for High-Stakes Decisions and Use Interpretable Models Instead*, 1 Nature Mach. Intell. 206, 206–15 (2019).

[30] R. Manche & M. Myakala, *Explainability in Healthcare AI: Ensuring Patient-Centered Care and Informed Consent*, 46 J. Med. Sys. 33, 33–47 (2022).

[31] Cary Coglianese & David Lehr, Regulating by Robot: *Administrative Decision Making in the Machine-Learning Era,* 105 Geo. L.J. 1147, 1164–67 (2017).

[32] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 168) 1.

[33] Danielle Keats Citron & Frank Pasquale, The *Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 12–15 (2014).

[34] Cyberspace Admin. of China, Provisions *on the Administration of Algorithmic Recommendation for Internet Information Services* (2022).

[35] NITI Aayog, *Responsible AI for All: Strategy for India* (2021).

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

[37] *Nilabati Behera v. State of Orissa*, (1993) 2 SCC 746 (India).

[38] *M.C. Mehta v. Union of India*, (1987) 1 SCC 395 (India).

[39] Andreas Matthias, *The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata*, 6 Ethics & Info. Tech. 175, 176–78 (2004).

[40] Luciano Floridi et al., *AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, 28 Minds & Machines 689, 697–703 (2018).