INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

REGULATING ARTIFICIAL INTELLIGENCE IN INDIA: A COMPARATIVE ANALYSIS OF LIABILITY, ACCOUNTABILITY, AND ALGORITHMIC BIAS UNDER THE EU AI ACT AND EMERGING GLOBAL FRAMEWORKS

AUTHORED BY - MANISH KUMAR SAHU

Assistant Professor, Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India

Abstract

Automated decision-making (ADM) systems now influence credit, hiring, welfare delivery, policing and adjudication. When these systems err or discriminate, existing legal doctrines built around human actors struggle to assign responsibility. This paper examines how India, the European Union and the United States allocate liability, demand accountability and address algorithmic bias in AI-driven decisions. India relies on a patchwork of constitutional guarantees, the Information Technology Act 2000, the Consumer Protection Act 2019 and the Digital Personal Data Protection Act 2023 (DPDP Act), none of which squarely regulates ADM. The EU has adopted a risk-based, ex ante regime in the AI Act (Regulation (EU) 2024/1689), complemented by the GDPR and a revised product liability directive. The United States remains fragmented, combining sectoral anti-discrimination statutes with emerging state legislation. Using doctrinal and comparative methods, the paper argues that India should adopt a proportionate, sector-sensitive framework that combines risk-based obligations for high-impact systems, a statutory right to explanation and human review, mandatory bias auditing, and a clear liability allocation across the AI value chain. It concludes with specific legislative and institutional recommendations.

Keywords: artificial intelligence; algorithmic bias; automated decision-making; liability; accountability; EU AI Act; DPDP Act 2023; India.

ISSN: 2582-6433

1. Introduction

1.1 Background

Algorithms increasingly decide who receives a loan, an interview, a welfare benefit or bail. Their appeal lies in speed, scale and apparent objectivity. Yet empirical studies show that automated systems can reproduce and amplify historical prejudice. Investigative reporting on the COMPAS recidivism tool found markedly different error rates across racial groups[1], and the 'Gender Shades' study documented significantly higher error rates for darker-skinned women in commercial facial analysis systems[2]. Such harms raise legal questions that traditional doctrines of negligence, contract and anti-discrimination law were not designed to answer: who is responsible when no human made the impugned decision, and how can an affected person contest a decision they cannot understand?

India is a particularly important site for this inquiry. The State is rapidly digitising welfare delivery, identity verification, policing and financial inclusion, while private actors deploy AI in lending, recruitment and insurance. At the same time, India has no dedicated AI statute. Its approach has so far been guided by policy documents, notably NITI Aayog's *Responsible AI* papers (2021) and subsequent government governance guidelines[3], rather than binding rules.

1.2 Statement of the Problem

Indian law lacks clear rules on (i) who bears legal responsibility for harm caused by AI-driven decisions, (ii) what transparency and contestability a person is entitled to when subjected to such decisions, and (iii) how algorithmic discrimination should be detected and remedied. Comparative frameworks, especially the EU's, offer instructive but imperfectly transferable models.

1.3 Research Questions

1. How does existing Indian law address liability, accountability and bias in automated decision-making, and where are its gaps?
2. How do the EU and US regimes allocate responsibility and regulate bias, and with what strengths and weaknesses?
3. What regulatory model should India adopt, given its constitutional commitments and institutional capacity?

1.4 Objectives

- To map the Indian legal framework applicable to AI-driven decisions.

ISSN: 2582-6433

- To critically analyse the EU AI Act, the GDPR's rules on ADM and the US approach.
- To identify transferable lessons and propose reforms for India.

1.5 Research Methodology

The paper uses **doctrinal** analysis of statutes, regulations and case law, and a **comparative** method that evaluates the three jurisdictions across common criteria: scope, risk classification, liability, transparency, bias mitigation and enforcement. Sources include primary legal texts, judicial decisions, official policy documents and peer-reviewed scholarship. The analysis is normative as well as descriptive, and culminates in reform proposals.

1.6 Scope and Limitations

The paper focuses on decision-making systems affecting individuals' legal or similarly significant interests (credit, employment, welfare, public administration). It does not address copyright in AI outputs, military AI, or deepfake-specific regulation. AI regulation is evolving quickly; the analysis reflects the position as understood at the time of drafting, and implementation timelines in particular should be re-checked.

1.7 Significance

The study contributes a comparative, India-focused account of ADM governance and offers concrete reform proposals for policymakers, regulators and practitioners.

2. Conceptual Framework and Literature Review

2.1 Key Concepts

Automated decision-making refers to decisions taken by technological means without meaningful human involvement. **Algorithmic bias** denotes systematic and unfair differential outcomes produced by a system, arising from skewed training data, flawed proxies, design choices or deployment context[4]. **Accountability** has both a forward-looking element (duties of design, testing and oversight) and a backward-looking one (answerability and remedy). **Liability** concerns the allocation of legal responsibility for harm.

2.2 The Opacity Problem

Pasquale[5] describes modern algorithmic systems as 'black boxes' whose internal workings are shielded from scrutiny by technical complexity and trade secrecy. Kroll and others[6] argue that accountability can be built into systems through technical means such as audit trails and

ISSN: 2582-6433

procedural regularity, rather than relying solely on after-the-fact explanation.

2.3 Disparate Impact and Proxy Discrimination

Barocas and Selbst[7] show that even without explicit use of protected characteristics, models can discriminate through correlated proxies, and that doctrines such as disparate impact fit awkwardly with data-mining practices. This is critical for India, where caste, religion, gender, language and region may be inferred from seemingly neutral data such as surnames, postal codes or consumption patterns.

2.4 The Explanation Debate

Wachter, Mittelstadt and Floridi[8] contend that the GDPR does not create a robust, general 'right to explanation' of individual automated decisions, instead offering a more limited right to information and safeguards. Subsequent case law and the AI Act have partly altered this picture (see Section 6).

2.5 Liability for Autonomous Systems

Abbott[9] argues that where AI performs better than humans, the law should evaluate its conduct by a standard of reasonable computer performance rather than reasonable human care. The wider debate centres on fault-based liability, strict liability and mandatory insurance as alternatives for harms where causation and fault are hard to prove.

2.6 Research Gap

Existing scholarship is dominated by EU and US perspectives. There is limited systematic analysis of how Indian constitutional and statutory law, including the DPDP Act 2023, handles ADM, and of which comparative features suit India's institutional context.

3. Liability and Accountability in AI-Driven Decisions: Theoretical Foundations

3.1 The Attribution Problem

AI harms typically involve many actors: data providers, model developers, system integrators, deployers and users. The 'many hands' problem and the opacity and adaptiveness of machine-learning systems make it difficult to prove breach, causation and foreseeability under conventional tort and contract law.

ISSN: 2582-6433

3.2 Models of Liability

- **Fault-based liability** (negligence) maintains familiar standards but burdens claimants with proving breach and causation in technically opaque settings.
- **Strict or product liability** shifts risk to producers and is suited to defective products, but its application to software and continuously learning systems is contested.
- **Reversal or alleviation of the burden of proof** and disclosure duties can address information asymmetry without abandoning fault.
- **Regulatory accountability** imposes ex ante duties (risk management, testing, documentation) enforced by administrative penalties.

3.3 Accountability Principles

Widely accepted principles include transparency, explainability proportionate to impact, human oversight, non-discrimination, data quality, robustness and effective redress. These principles inform the comparative assessment that follows.

4. Algorithmic Bias: Legal Dimensions

Bias enters at several stages: problem formulation, data collection, labelling, feature selection, model training and deployment. Legal responses therefore need to operate across the lifecycle rather than only at the point of decision. Three recurring difficulties arise.

First, **proof**: victims rarely have access to the data or code needed to demonstrate discrimination. Second, **intent**: doctrines requiring discriminatory intent are ill-suited to statistical systems, which discriminate without any human intending it. Third, **remedy**: even when bias is shown, it is unclear whether the remedy lies against the developer, the deployer or both.

Litigation illustrates these tensions. In *State v Loomis* 881 NW 2d 749 (Wis 2016), the Wisconsin Supreme Court permitted use of a proprietary risk assessment at sentencing subject to cautions[10], despite the defendant's inability to examine the algorithm. In the employment context, *Mobley v Workday* in the Northern District of California has tested whether an AI vendor may face liability as an 'agent' of employers for allegedly discriminatory screening[11]; readers should check its current procedural status.

ISSN: 2582-6433

5. The Indian Legal Framework

5.1 Constitutional Foundations

There is no AI-specific legislation in India, but the Constitution supplies strong normative anchors.

Equality (Article 14, 15). The Supreme Court's recognition that arbitrariness violates Article 14 (*E P Royappa v State of Tamil Nadu* (1974) 4 SCC 3; *Maneka Gandhi v Union of India* (1978) 1 SCC 248) provides a basis to challenge opaque or arbitrary algorithmic State decisions. Discrimination on prohibited grounds under Article 15 applies to State action, including action mediated by algorithms.

Privacy and dignity (Article 21). In *Justice K S Puttaswamy v Union of India* (2017) 10 SCC 1, a nine-judge bench held privacy to be a fundamental right and recognised informational privacy and autonomy. The proportionality test in *Puttaswamy* and its Aadhaar decision (*Justice K S Puttaswamy (Aadhaar) v Union of India* (2019) 1 SCC 1) requires legitimate aim, suitability, necessity and balancing, a framework readily applicable to State deployment of automated systems such as facial recognition or welfare-eligibility algorithms.

Fair procedure. Principles of natural justice, including reasoned decisions and the opportunity to be heard, are difficult to satisfy when decisions are generated by opaque models, an argument that litigants and courts will increasingly face.

5.2 Information Technology Act 2000

The IT Act addresses intermediaries, cybercrime and electronic records, but was not designed for generative or decision-making AI. Section 79 offers intermediaries conditional safe harbour[12]; whether AI developers or deployers qualify as intermediaries for AI-generated outputs is unsettled. Section 43A, which concerned compensation for failure to protect sensitive personal data, has been superseded in practice by the DPDP Act[13].

5.3 Digital Personal Data Protection Act 2023

The DPDP Act is India's first comprehensive data protection statute. It establishes obligations for data fiduciaries (notice, consent or specified legitimate uses, purpose limitation, accuracy, security, breach notification), rights for data principals (access to information, correction and erasure, grievance redressal, nomination), and a Data Protection Board. Its main limitations for ADM are:

- **No express right against solely automated decisions** and no right to meaningful explanation comparable to Article 22 GDPR.

ISSN: 2582-6433

- **Broad State exemptions and legitimate uses** (sections 7 and 17)[14], which cover much public-sector automated decision-making, including welfare and security functions.
- **Limited bias-specific duties**: data accuracy and completeness obligations apply where data is used to make a decision affecting the data principal, but there is no mandatory impact assessment or audit for ordinary fiduciaries.
- **Limited scope**: it covers personal data only, leaving model risk arising from non-personal or anonymised data unaddressed.

The DPDP Rules, notified in late 2025[15], operationalise the Act through phased commencement; their timelines should be verified.

5.4 Consumer and Tort Law

The Consumer Protection Act 2019 introduces a product liability regime (Chapter VI)[16] covering manufacturing defects, design defects and failure to warn, and recognises unfair trade practices and 'service' deficiencies. These provisions may reach AI-enabled products and services, but their fit with software, continuously learning models and distributed supply chains has not been tested by courts. Under general tort law, claimants must prove duty, breach and causation, a heavy burden given opacity. Criminal liability for negligent acts causing death under the Bharatiya Nyaya Sanhita 2023 may apply to human actors[17], but offers little guidance for autonomous system failures.

5.5 Sectoral and Policy Instruments

Sectoral regulators have issued piecemeal guidance, for example on algorithmic and AI use in financial services. At the policy level, NITI Aayog's *Responsible AI* papers (2021) articulated principles of safety, equality, inclusivity, transparency, accountability and protection of values[18], while the Ministry of Electronics and Information Technology (MeitY) has since moved toward AI governance guidelines favouring a principles-based, innovation-friendly approach over a standalone statute. These instruments are non-binding and lack enforcement mechanisms.

5.6 Assessment

Indian law provides powerful constitutional principles but weak operational rules. Rights are enforceable mainly against the State through writ jurisdiction; private-sector ADM falls into gaps between data, consumer and tort law. There is no mandated transparency, no bias auditing

ISSN: 2582-6433

duty, and no allocation of liability across the AI supply chain.

6. The European Union Framework

6.1 The AI Act (Regulation (EU) 2024/1689)

The AI Act is the world's first comprehensive horizontal AI statute. It entered into force on 1 August 2024[19] with staggered application: prohibitions from February 2025, general-purpose AI obligations from August 2025, and most high-risk obligations originally from August 2026. The Commission's 2025 'digital omnibus' proposals sought to defer some high-risk obligations; the final timetable should be verified.

Risk-based architecture. The Act prohibits certain practices (for example social scoring and some forms of manipulative AI and biometric categorisation), imposes extensive obligations on **high-risk systems** (including those used in employment, education, essential services such as credit scoring, law enforcement, migration and administration of justice, listed in Annex III[20]), and sets transparency duties for limited-risk systems such as chatbots.

Provider obligations for high-risk systems include a risk management system (Article 9), data governance with attention to bias in training, validation and testing data (Article 10), technical documentation and logging (Articles 11 to 12), transparency and instructions for use (Article 13), human oversight (Article 14), accuracy, robustness and cybersecurity (Article 15), and conformity assessment and post-market monitoring[21].

Deployer obligations (Article 26) include using systems per instructions, assigning competent human oversight, monitoring operation and, for certain deployers, conducting a fundamental rights impact assessment (Article 27)[22].

Right to explanation. Article 86 grants persons affected by decisions based on certain high-risk systems a right to obtain clear and meaningful explanations of the system's role and main elements of the decision[23].

Enforcement. Market surveillance authorities and the AI Office oversee compliance, with administrative fines reaching up to EUR 35 million or 7 per cent of worldwide turnover for the most serious infringements (Article 99)[24].

6.2 GDPR and Automated Decisions

Article 22 GDPR gives individuals the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects, subject to exceptions and safeguards including human intervention[25]. In *SCHUFA Holding (Scoring)* (Case C-634/21, 7 December 2023), the Court of Justice held that the generation of a credit score can

ISSN: 2582-6433

itself constitute an automated 'decision' where a third party draws strongly on it, which significantly widened Article 22's reach and addressed a gap where the scoring agency and the lender were different entities[26].

6.3 Liability

The revised Product Liability Directive (Directive (EU) 2024/2853) expressly extends strict liability to software, including AI systems, and eases claimants' burden through disclosure obligations and rebuttable presumptions of defect and causation in complex cases[27]. A separate proposal for an AI Liability Directive, which would have addressed fault-based claims, was withdrawn by the Commission in 2025[28], leaving national tort law to govern non-product claims.

6.4 Assessment

The EU model is comprehensive and rights-oriented, and it targets the lifecycle through ex ante duties. Criticisms include compliance cost for smaller firms, definitional breadth, reliance on harmonised standards still under development, and the risk that procedural compliance substitutes for substantive fairness.

7. The United States Framework

The US has no comprehensive federal AI statute. Regulation proceeds through:

- **Existing anti-discrimination law**, including Title VII of the Civil Rights Act (employment), the Equal Credit Opportunity Act and Fair Housing Act[29], applied through disparate treatment and disparate impact theories. Federal agencies have asserted that these laws apply to automated systems, although the enforcement posture has shifted with changes in administration.
- **Sectoral and consumer protection law**, such as the Fair Credit Reporting Act and Federal Trade Commission authority over unfair or deceptive practices[30].
- **State and local laws**, such as New York City Local Law 144 of 2021 (bias audits of automated employment decision tools)[31] and the Colorado AI Act (SB 24-205)[32], which imposes duties of reasonable care on developers and deployers of high-risk systems to prevent algorithmic discrimination. Implementation timelines for state laws have been revised and are subject to federal pre-emption debates.
- **Non-binding frameworks**, notably the NIST AI Risk Management Framework (2023), which has become an influential voluntary standard[33].

ISSN: 2582-6433

Liability is largely governed by state tort and product law, with open questions on whether software is a 'product' and on vendor liability for discriminatory outcomes. The strengths of the US model are flexibility and innovation-friendliness; weaknesses are fragmentation, uneven protection, and heavy reliance on private litigation, which struggles with opacity and the intent requirement.

8. Comparative Analysis

Criterion	India	European Union	United States
Legislative approach	No AI statute; policy guidelines, general laws	Horizontal, risk-based AI Act plus GDPR	Fragmented: sectoral federal law, state laws, voluntary standards
Risk classification	None binding	Prohibited, high-risk, limited, minimal	Varies by state and sector
Right to explanation / human review	None general; limited DPDP rights	Art 22 GDPR; Art 86 AI Act; human oversight duties	Limited; sector-specific adverse action notices
Bias mitigation duties	Not mandated	Data governance and testing duties; fundamental rights assessments	Bias audits in some jurisdictions; anti-discrimination statutes
Liability	General tort, consumer law; untested	Strict product liability extended to software; national fault rules	State tort and product law; uncertain for software
Enforcement	Writs against State; Data Protection Board	Market surveillance authorities; heavy fines	Agencies, state attorneys general, private suits

Observations. First, the EU offers the most complete accountability architecture but at high compliance cost. Second, the US shows both the value of sectoral anti-discrimination enforcement and the limits of a patchwork. Third, India's greatest strength is its constitutional jurisprudence on privacy, equality and proportionality; its greatest weakness is the absence of operational duties and enforcement capacity. Direct transplantation of the EU model risks overburdening India's start-up ecosystem and regulators, while the US model's fragmentation would leave most Indians without effective protection.

ISSN: 2582-6433

9. Recommendations for India

1. **A proportionate, risk-based framework.** Enact a statute or amend existing law to regulate high-impact AI systems (credit, employment, insurance, welfare, policing, health, education), with lighter obligations for low-risk uses.
2. **A statutory right to explanation and human review.** Individuals subject to significant automated decisions should be entitled to notice that AI was used, a meaningful explanation of its role and key factors, and a right to human reconsideration. The DPDP Act or its rules could be amended for this purpose.
3. **Mandatory impact assessments and bias audits.** Require algorithmic impact assessments for high-risk deployments, and independent bias audits where decisions affect protected groups, tailored to Indian axes of disadvantage including caste, religion, gender, disability, language and region.
4. **Narrow the public-sector exemptions.** State use of ADM should meet the *Puttaswamy* proportionality test, with legislative authority, transparency and independent oversight, rather than blanket exemptions.
5. **Clear liability allocation across the value chain.** Clarify the respective duties of developers, deployers and operators; extend product liability expressly to software; adopt disclosure duties and rebuttable presumptions of causation where claimants cannot access technical evidence.
6. **A competent regulator and technical capacity.** Establish or designate an AI regulator or coordinated body with technical expertise, working with sectoral regulators (RBI, SEBI, IRDAI) and the Data Protection Board, and supported by regulatory sandboxes and standards bodies.
7. **Proportionality for small enterprises.** Offer phased compliance, safe harbours for good-faith compliance with recognised standards, and support for start-ups to avoid entrenching incumbents.
8. **Documentation and traceability.** Mandate logging and record-keeping for high-risk systems to enable post-incident investigation and redress.
9. **Accessible redress.** Provide expedited complaint mechanisms, collective actions and legal-aid support, recognising the practical barriers faced by affected individuals.

ISSN: 2582-6433

10. Limitations and Directions for Future Research

This paper relies on doctrinal and secondary analysis and does not include empirical evidence on Indian ADM deployments. The regulatory landscape is moving quickly: EU timelines, US federal and state developments and Indian policy may have changed since drafting. Future research could examine sector-specific regimes (for example credit and welfare), judicial use of AI, the interaction of ADM with caste-based discrimination, and enforcement experience under the AI Act.

11. Conclusion

AI-driven decision-making challenges legal systems built on human agency, intent and visible reasoning. India's constitutional jurisprudence provides a principled foundation, but its statutory framework does not yet translate those principles into operational duties or accessible remedies. The EU AI Act offers a rigorous, lifecycle-based model, while the US experience demonstrates both the strengths and limits of sectoral enforcement. A context-sensitive Indian framework, built on risk-proportionate obligations, explanation and human review rights, bias auditing, clear liability allocation and capable institutions, can protect individuals without stifling innovation. Delay carries its own risk: as automated decisions become embedded in public and private life, the cost of retrofitting accountability will only rise.

Notes

[1] Julia Angwin and others, 'Machine Bias' (*ProPublica*, 23 May 2016).

[2] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77.

[3] NITI Aayog, *Responsible AI for All: Approach Document for India* (2021).

[4] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.

[5] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

[6] Joshua A Kroll and others, 'Accountable Algorithms' (2017) 165 University of Pennsylvania Law Review 633.

[7] Barocas and Selbst (n 4).

[8] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017)

ISSN: 2582-6433

7 International Data Privacy Law 76.

[9] Ryan Abbott, 'The Reasonable Computer: Disrupting the Paradigm of Tort Liability' (2018) 86 George Washington Law Review 1.

[10] *State v Loomis* 881 NW 2d 749 (Wis 2016).

[11] *Mobley v Workday Inc* (ND Cal, filed 2023).

[12] Information Technology Act 2000, s 79.

[13] Information Technology Act 2000, s 43A; Digital Personal Data Protection Act 2023, s 44.

[14] Digital Personal Data Protection Act 2023, ss 7, 17.

[15] Digital Personal Data Protection Rules 2025.

[16] Consumer Protection Act 2019, ch VI.

[17] Bharatiya Nyaya Sanhita 2023.

[18] NITI Aayog (n 3).

[19] Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L, art 113.

[20] ibid arts 6, annex III.

[21] ibid arts 9–15, 43, 72.

[22] ibid arts 26–27.

[23] ibid art 86.

[24] ibid art 99.

[25] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 22.

[26] Case C-634/21 *SCHUFA Holding (Scoring)* EU:C:2023:957.

[27] Directive (EU) 2024/2853 of the European Parliament and of the Council on liability for defective products [2024] OJ L.

[28] European Commission, *Commission Work Programme 2025* COM(2025) 45 final.

[29] Civil Rights Act 1964, Title VII, 42 USC § 2000e et seq; Equal Credit Opportunity Act, 15 USC § 1691 et seq; Fair Housing Act, 42 USC § 3601 et seq.

[30] Fair Credit Reporting Act, 15 USC § 1681 et seq; Federal Trade Commission Act, 15 USC § 45.

[31] New York City Local Law 144 of 2021.

[32] Colorado Artificial Intelligence Act, SB 24-205 (2024).

[33] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023).

ISSN: 2582-6433

Bibliography

Cases

E P Royappa v State of Tamil Nadu (1974) 4 SCC 3

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

Justice K S Puttaswamy (Aadhaar) v Union of India (2019) 1 SCC 1

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

Mobley v Workday Inc (ND Cal, filed 2023)

SCHUFA Holding (Scoring) (Case C-634/21) EU:C:2023:957

State v Loomis 881 NW 2d 749 (Wis 2016)

Legislation and Regulations

Bharatiya Nyaya Sanhita 2023 (India)

Colorado Artificial Intelligence Act, SB 24-205 (2024)

Consumer Protection Act 2019 (India)

Constitution of India 1950, arts 14, 15, 21

Digital Personal Data Protection Act 2023 (India)

Directive (EU) 2024/2853 of the European Parliament and of the Council on liability for defective products [2024] OJ L

Information Technology Act 2000 (India)

New York City Local Law 144 of 2021

Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1

Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L

Secondary Sources

Abbott R, 'The Reasonable Computer: Disrupting the Paradigm of Tort Liability' (2018) 86 George Washington Law Review 1

Angwin J and others, 'Machine Bias' (*ProPublica*, 23 May 2016)

Barocas S and Selbst A, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671

Buolamwini J and Gebru T, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77

Kroll J and others, 'Accountable Algorithms' (2017) 165 University of Pennsylvania Law Review 633

NITI Aayog, *Responsible AI for All: Approach Document for India* (2021)

National Institute of Standards and Technology, *Artificial Intelligence Risk Management*

ISSN: 2582-6433

Framework (AI RMF 1.0) (2023)

Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015)

Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76