Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 18 (01), 2026
pp. 242 - 255

Aligning AI Regulatory Approaches: Multi- Layered Frameworks and Social Justice in the EU, US, and India

[1]Dr. Vibhuti Jaswal, [2]Shiekhar Panwar

Assistant Professor of Law, School of Law, SVKM's Narsee Monjee Institute of Management Studies (NMIMS), Chandigarh Campus.

Independent Transactional Lawyer, Dehradun, Uttarakhand.

Abstract:

The review article examines the comparative governance of artificial intelligence (AI) in the European Union, the United States, and India, focusing on various issues such as liability, bias, privacy, and AI use in judicial processes, while attending to legal, ethical, and social justice considerations. There are distinct regulatory strategies for the working of AI systems. in each jurisdiction. The EU has introduced a comprehensive AI Act with a risk- based, rights-oriented regime. The United States relies on a decentralized, agency-led model grounded in sectoral oversight and standards. India, is still formulating AI governance guidelines that emphasizes on the areas of innovation and inclusion. Despite these divergent frameworks, common concerns emerge around ensuring algorithmic accountability, protection of privacy and individual rights, preserving public trust, and preventing any discriminatory outcomes. Based on these outcomes, the paper proposes a novel multi-layered regulatory framework that deals with the integration of statutory regulation, ethical guidelines, and oversight mechanisms across different levels of governance. This approach harmonizes substantive aspect with practicality, balances innovation with accountability, and embeds ethical and social justice principles into AI regulation. By bridging these dimensions, the framework aims to ensure robust framework on liability, mitigation of bias efficiently, protection of data privacy, and responsible use of AI in judicial arena. The comparative analysis emphasize the need for cohesive AI governance that adapts to different legal systems along with the upholding common principles of justice and accountability.

Keywords: Algorithmic Accountability; Social Justice; AI regulation; EU AI Act; U.S. Agency model; India AI governance

Received: 6 November 2026 **Revised**: 22 December 2026 **Accepted:** 31 December 2026

1. Introduction

Artificial Intelligence (AI) is advancing rapidly across various sectors and jurisdictions thereby increasing the need of urgent debates and discussions about the governance of the impact. Algorithmic decision-making has become one of the "hot emerging" legal issue that demands solutions for innovative governance. Autonomous systems faces new challenges such as onus of liability, algorithmic bias and discrimination, data privacy, and even the use of AI by courts. Traditional legal frameworks are difficult to be implemented because of the combination of challenges and opacity and autonomy.[1] At present, in India there is no existing legislation on artificial intelligence but partially covered in laws relating to data or consumer protection. The issues which these legislations deal with are partially about bias, safety, and accountability.[2]

[1] Legacy Law Offices. "AI on Trial: Rethinking Liability in India's Current Legal Framework." Legacylawoffices.com, 9 September 2025. https://www.legacylawoffices.com/ai-on-trial-rethinking-liability-in-indias-current-legal-framework/.

[2] Pandey, Swaraj. "Regulation of Artificial Intelligence in India: Legal Challenges and Policy Recommendations." SSRN Electronic Journal, 2025. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5358959#:~:text=the%20few%20developing%20countries%20receiving,T

Similarly, the United States has no single AI statute, and European Union than relying on patchwork sectoral rules, has adopted a comprehensive framework.[3]

One of the key developments is the European Union's 2024 risk-based AI Act, which has introduced a multi-layered framework of rules especially the segregation of AI systems on the basis of risk. The EU model bans the "unacceptable risk" of the AI system when used which is most harmful. Strict requirements have been imposed on the use of "high-risk" systems such as in the field of healthcare, transport, employment, policing, or justice. The regulation provides the mandate for transparency to be followed in the applications where the risk level is low.[4] The act has adopted the tiered approach , the higher the risk, the stricter the rules aims to ensure AI is safe, transparent, and non-discriminatory and not infringing the fundamental rights.[5] The EU's comprehensive strategy draws a distinction from a more fragmented U.S. approach and the emerging legislative frameworks in India.[6] It provides an innovative approach through the adoption of multi-layered regulatory framework.

The AI regulations must focus on the principles of algorithmic accountability and social justice, if unchecked then it can harm the vulnerable communities. For instance, if AI models are trained on biased data can portray discriminatory output by targeting structural racism, vulnerable groups and inequality. In India, if AI discrimination is unaddressed, it can be either against caste, class or gender. There have been cases where autonomous systems such as facial recognition technology or predictive policing model has impacted the minority section of people on the grounds of colour or gender. These realities highlight the need for algorithmic fairness, transparency, and accountability as core principles of AI governance. As social justice is impacted because of the discriminatory nature of AI, the banning of the use is being promoted. Example, U.S. cities have begun banning police use of facial recognition technology. Various AI

The paper proposes a comparative, multi-layered regulatory approach to AI, by comparing the frameworks of European Union, the United States, and India. It is in reference to the addressing of or which should be addressed focusing on four key fronts: liability for AI-caused harms, algorithmic bias, data privacy, and the use of AI in judicial processes.[7] A regulatory framework must be framed that balances innovation with ethics and human rights. The comparative framework is combination of the EU's rigorous framework, the U.S.'s sectoral initiatives, and India's constitutional values converging into a robust "algorithmic accountability" regime.[8]

2. Liability of AI Systems

The question igniting the fiery debates is the arena of liability shall lie on whom in case the harm is caused by AI systems. The black box nature of AI complicates the role of assigning the responsibility under the traditional tort.

European Union:

As EU has introduced AI regulation focusing on tiered approach of AI systems while focusing on updating it regarding product liability laws for covering the AI aspect. A draft AI Liability Directive (AILD) will make it easy to deal with the fault-based claims for damage caused by AI inclusive of harms caused from safety breaches or unlawful discrimination by algorithms.[9] Strict liability is favored for high-risk AI systems by

his%20study%20examines%20other.

[3] Ibid at 1.

[4] RAND Corporation. Developing Effective Governance for Synthetic Data and Generative AI Systems. Santa Monica, CA: RAND, 2025. https://www.rand.org/pubs/research_reports/RRA3243-3.html.

[5] Norton Rose Fulbright. "Artificial Intelligence and Liability." Nortonrosefulbright.com, 2025. https://www.nortonrosefulbright.com/en/knowledge/publications/7052eff6/artificial-intelligence-and-liability.

[6] RAND Corporation. Developing Effective Governance for Synthetic Data and Generative AI Systems. Santa Monica, CA: RAND Corporation, 2025. https://www.rand.org/pubs/research_reports/RRA3243-3.html.

[7] American Civil Liberties Union. "AI Could Exacerbate Inequality, Experts Warn." Aclu.org, 22 July 2025. https://www.aclu.org/news/privacy-technology/ai-could-exacerbate-inequality-experts-warn.

[8] Tiwari, Shreya. "Towards Rights-Based AI Framework In India: Bridging Global Models And Constitutional Duties." Livelaw.in, 26 July 2025. https://www.livelaw.in/lawschool/articles/towards-rights-based-ai-framework-india-bridging-global-models-constitutional-duties-298896.

[9] Norton Rose Fulbright. "Artificial Intelligence and Liability." Nortonrosefulbright.com, 2024. https://www.nortonrosefulbright.com/en/knowledge/publications/7052eff6/artificial-intelligence-and-liability.

making providers of high-risk AI systems liable for harm regardless of fault. The principle of accountability and customer safety is of utmost importance while protecting the victim against the harm caused by AI. If any form of injury or loss caused by AI algorithm then the provider must be made liable. If the victim is left with no remedy, then it will lead to denial of access to justice. Civil liability is indirectly dealt by framing rigorous compliance standards for high-risk AI systems. EU AI Act combines ex ante regulation with adapted ex post liability rules to ensure there are appropriate recourses and incentives for safe AI development.[10] By making AI providers and deployers more accountable, the EU framework aims to internalize the social costs of AI harms and thus encourage "responsible innovation."[11]

United States:

United States has adopted a decentralized approach to the concept of AI liability. As there is no existing federal AI liability statute, so different industries have adopted their own application of standards. Traditional U.S. liability doctrines can be applied but the uncertainty amongst court exists for the issues of autonomous decision making. And the consequence of the same has been the rise in AI bills (around 90 pieces) being drafted by the Congress focusing on various aspects of AI risk. Some bills seek to designate an AI regulator or impose transparency and evaluation requirements, while others propose liability safeguards to protect the rights of consumers. However, the emphasis of such draft legislations is on a certain kind of liability and not broad liability. U.S. relies on the system of combination of general existing laws and specific subject area framework. Specific sectoral regulation will vary liability rules based on the facts and circumstances of the case. As in the case of Amazon AI recruitment algorithm case, where men were preferred over females during shortlisting, specific employment framework and respective state law was applied. The following approach prioritizes flexibility and innovation by avoiding blanket rules but may leave victims without clear remedies. Taking the above example the situation of liability is unclear that who is to be sued.[12] If yes, under what framework the rights of the victim are going to be protected. Policymakers are debating upon the issue either to to move toward strict liability for certain high-risk AI or to maintain a fault-based approach that might help protect the tech developers and startups. The status quo in the U.S. adopted can be described as "liability by analogy" where the courts and regulators are trying to fit AI into existing legal framework., an approach that may prove insufficient as AI becomes more complex.

India:

The present framework provides only fragmented coverage of AI related harms. The general laws such as Digital Personal Data Protection Act 2023, Information Technology Act, 2000 and Consumer Protection Act, 2019 deals with personal data, cybersecurity and online harms and defective products or deficient services respectively. These legislations are general in nature and not focused on AI specific tailored to the scenario of an autonomous AI system causing damage.[13] The challenges of autonomous and opaque systems are not addressed by the present legislative framework. The question arises what if a delivery drone causes injury or the diagnostic tool gives wrong result thereby causing harm to the victim; the liability perspective is unclear whether it falls on the software developer, the company deploying the AI, or even the end-user who operated it. As there is no specific law on artificial intelligence courts have resorted to the application of principles of product liability, negligence, or even constitutional rights. There is a growing recognition in India that a tailored AI liability regime is the need of the hour. Recently, the government launched an IndiaAI Mission and an AI Safety & Ethics Institute to study standards for safe AI.[14] Policy experts are debating options: for example, whether India should adopt a strict liability rule for high-risk AI (ensuring

[10] Regulation (EU) 2016/679 (GDPR), art 22.

[11] European Parliamentary Research Service. Artificial Intelligence and Liability for the Purposes of Civil Liability. Brussels: European Parliament, 2023. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.

[12] Ajoy. "Artificial Intelligence and the Courts." Clpr.org.in, 2021. https://clpr.org.in/blog/artificial-intelligence-and-the-courts/.

[13] Tiwari, Shreya. "Towards Rights-Based AI Framework In India: Bridging Global Models And Constitutional Duties." Livelaw.in, 26 July 2025. https://www.livelaw.in/lawschool/articles/towards-rights-based-ai-framework-india-bridging-global-models-constitutional-duties-298896

[14] Ministry of Electronics and Information Technology. India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation. New Delhi: Government of India, 2025. https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf.

consumer protection) versus a more innovation friendly stance that requires proving fault. The comparative outlook provides guidance.[15]

The EU's approach of clear accountability is attractive from a consumer safety perspective, whereas the U.S. illustrates the pitfalls of a patchwork approach.[16] Without legal clarity, victims suffering from harm caused by AI in India, could fall into a remedial black hole. Thus, aligning with a multilayered framework would mean India enacting laws that define roles (developer vs. deployer liability), mandate risk-mitigating steps (testing, disclosures), and provide avenues for redress (perhaps special AI tribunals or insurance schemes). Indeed, commentators argue that India urgently needs a "forward-looking AI liability regime" that balances innovation with accountability. Liability is a cornerstone of algorithmic accountability. The EU's risk-tiered model and proposed strict liabilities represent the top layer of protection by putting the onus on those best placed to prevent harm. The U.S. approach, while decentralized, shows the value of sector-specific expertise but is moving toward more oversight as AI risks grow. India, currently without a dedicated regime, stands to benefit by bridging these models by implementing a hybrid that imposes strict liability for especially harmful uses (echoing EU's stance on high-risk AI) while building in flexibility for innovation. A multi-layered framework would ensure that from developers to deployers, every actor in the AI value chain has clear legal responsibilities, and those affected by AI failures have a path to remedies.

3. Algorithmic Bias and Fairness

Automated systems systematically discriminate or produce unfair outcomes by inducing risk through output creating AI bias. It has become one of the most prominent social justice concerns in AI governance. Because AI algorithms learn from historical data, they can inadvertently perpetuate existing biases based on race, gender, class, or other protected characteristics. All three jurisdictions have grappled with how to ensure fairness, non-discrimination, and transparency in AI:

European Union:

The EU's AI regulation explicitly seeks to prevent "unlawful biases" and discriminatory impacts from AI systems. The AI Act mandates that high-risk AI systems be designed and trained in a manner that respects fundamental rights, including the prohibition of discrimination as enshrined in the EU Charter of Fundamental Rights.[17] For example, Article 10 of the Act requires the providers of high-risk AI models to use training data that is relevant, representative, and free of errors "to the best extent possible".[18] The rationale behind it is to assess and mitigate biases in data sets. Few AI practices are outright banned under Article 5 of the Act due to their biased or manipulative nature for instance, AI systems that deploy subliminal techniques to exploit vulnerabilities of specific groups, or government-run social scoring systems that could discrimination in access to services. The EU's approach is preventive in nature by requiring rigorous data governance, documentation, and human oversight for high-risk AI, it aims to weed out bias before it causes harm. Additionally, the EU has broader frameworks buttressing algorithmic fairness. The GDPR's provisions (notably Article 22) give individuals the right not to be subject to purely automated decisions with significant effects, or at least the right to a human review and an explanation.[19] This reflects a European skepticism of unchecked algorithms and a commitment to human-in-the-loop decision-making to catch biases or errors. The new Framework Convention on AI and Human Rights being drafted by the Council of Europe likewise emphasizes non-discrimination and fairness as core principles. In summary, the EU is embedding fairness at multiple layers: specific AI rules, data protection law, and overarching human rights instruments all act in concert to identify, correct, and ultimately prohibit biased AI outcomes. The EU even sees potential in using AI against bias by. encouraging research into debiasing

[15] Canca, N. C., and E. Quintais. "Human Oversight Requirements for AI Decision-Making." Computer Law & Security Review 49 (2023). https://www.sciencedirect.com/science/article/pii/S0267364923000432.

[16] Government of Iceland. "Joint Nordic Statement: Artificial Intelligence and the Global Dialogue on AI Governance." Government.is, 19 February 2025. https://www.government.is/diplomatic-missions/embassy-article/2025/02/19/Joint-Nordic-Statement-Artificial-Intelligence-and-the-Global-Dialogue-on-AI-Governance/.

[17] DLA Piper. "Fairness / Unlawful Bias in the European Union." Intelligence.dlapiper.com, 2025. https://intelligence.dlapiper.com/artificial-intelligence/?t=10-fairness-or-unlawful-bias&c=EU.

[18] Regulation (EU) 2024/1689, art 10(2)(f), (5).

[19] Regulation (EU) 2016/679 (GDPR), art 22.

algorithms and viewing data transparency as a tool to fight discrimination but under strict governance.

United States:

In the absence of a unified national AI law, the U.S. addresses algorithmic bias through a mix of laws such as anti-discrimination law, guidance from various agencies, and local initiatives. Existing civil rights laws (like the Equal Credit Opportunity Act, Fair Housing Act, or employment discrimination laws) apply to AI-driven decisions also. For instance, if a lending algorithm disproportionately rejects loan applicants from a certain race, then fair lending laws are violated. Regulators such as the EEOC and FTC have warned that by using biased AI tools can be contrary to laws against disparate impacts. A well-known study found the COMPAS criminal risk assessment tool used in U.S. courts was biased towards Black defendants by falsely flagging them as a high-risk at much higher rates than white defendants. This revelation in 2016 prompted widespread concern that algorithmic tools could reinforce racial bias in sentencing and bail decisions. Likewise, audits of AI used in hiring have found gender or racial biases leading to calls for algorithmic audits. In response, a few jurisdictions enacted targeted laws such as New York City (requires bias audits of AI hiring tools), and Illinois and other states have laws addressing bias in AI video interviews. At the federal level, policy moves include the "AI Bill of Rights" Blueprint (2022) which, while not binding, articulated principles of equity and antidiscrimination. Recent executive orders are urging agencies to ensure AI advances civil rights.[20] Meanwhile, various Congressional bills on algorithmic accountability have been proposed (e.g. the Algorithmic Accountability Act) that would mandate impact assessments for biases in high-risk AI systems.[21] These efforts echo a common ground which are transparency and oversight further needed to reveal and fix biases. Civil liberties groups like the ACLU underscore that without transparency, AI can disproportionately harm marginalized communities for example, predictive policing algorithms trained on biased crime data will unfairly target minority neighborhoods, creating a vicious cycle.[22] This has led some U.S. cities such as Boston, to ban law enforcement's use of facial recognition technology, citing high error rates for women and people of color. In essence, the U.S. approach to AI bias is emerging as a patchwork of "algorithmic accountability" measures by encouraging voluntary AI ethics frameworks in industry, employing existing anti-bias laws to specific cases, and introducing new rules in domains like credit, employment, or policing. While not as unified as the EU, the direction is like to prevent harm to vulnerable groups, demand explainability, and insist on human accountability for automated decisions. Social justice advocates in the U.S. consider the steps as crucial so that AI "does not deepen the digital divide or exacerbate the racial wealth gap" but instead is harnessed to promote equitable outcomes.[23]

India:

The concerns about algorithmic bias are important in India's socio-economic context, given the country's diverse and stratified society. However, India currently lacks a dedicated legal mechanism to prevent or redress bias in AI-driven decisions and there have been instances of bias. AI systems are trained on historical data risk discrimination against caste, religious, or gender minorities in India for example, the Delhi Police's experimental predictive policing system (CMAPS) was found to disproportionately surveil minority neighborhoods.[24] Similarly, during the COVID-19 lockdown, some AI- based remote exam proctoring tools allegedly flagged students from marginalized communities more often for "suspicious behavior," perhaps due to differences in environmental or behavioral cues.[25]

These anecdotes illustrate a real risk of AI-fueled inequality in areas like welfare, law enforcement, education, and finance. Yet, if an individual in India is denied a welfare benefit or a loan due to a biased algorithm, no clear legal remedy exists. The Constitution of India guarantees equality and prohibits discrimination, but applying those principles to algorithmic decisions cannot be done without any present

[20] White House Office of Science and Technology Policy, Blueprint for an AI Bill of Rights (2022).
[21] White House OSTP, Blueprint for an AI Bill of Rights (Oct. 3, 2022).
[22] ACLU, Accountability in Artificial Intelligence (2025).
[23] ACLU Policy Brief, Artificial Intelligence and Racial Injustice (2024).
[24] Vidhi Centre for Legal Policy, "India's Tryst With Predictive Policing" (2021).
[25] DPDP Act, 2023, s 4; IndiaAI Governance Guidelines 2025, Sutra 3.

legislation. A rights-based AI framework in India that would explicitly prohibit discriminatory AI outcomes and grant individuals' rights to transparency, explanation, and appeal against automated decisions. The framework will help in adjudication of automated systems on the grounds of non- discrimination and meaningful human oversight. Notably, the EU AI Act's risk-based classification and its provision (Article 86) giving individuals a right to a justification for AI-involved decisions are cited as precedents. To fill the vacuum, interim steps in India include relying on existing laws (for instance, using constitutional writs to challenge arbitrary automated decisions by government) or sectoral guidelines (the Reserve Bank of India has issued fairness guidelines for AI in digital lending, etc.). The Digital Personal Data Protection Act 2023 also indirectly contributes by forbidding misuse of personal data, which intersects with fairness (e.g. disallowing processing of sensitive personal data that could be substitute for bias without consent).[26] On analysis, the DPDP Act fails to address critical AI-specific challenges like black-box decision-making and algorithmic discrimination. Therefore, aligning with a multi-layered approach for India means building new legal safeguards against algorithmic bias. This could involve requiring bias audits for AI systems used in high stakes public services, mandating algorithmic impact assessments for government AI projects, and establishing grievance redress mechanisms for citizens affected by AI (for example, an AI ombudsman or appellate tribunal). The AI Governance Guidelines 2025 emphasize fairness, inclusivity, and non-discrimination as key principles, and propose measures like requiring AI systems to undergo bias testing and documentation especially in sensitive sectors. It aligns with international best practices and the constitutional ethos of social justice. algorithmic bias is essential for AI governance that upholds social justice.[27]

The EU's robust rules ensure that fairness is roasted into AI design and deployment, which is backed by the force of law. The U.S. is increasingly vigilant about AI's civil rights impacts, although through a mosaic of laws and policies. India, with its diverse population, has much at stake because of the impact created on rights and is poised to craft a framework that could draw on both its own constitutional values and global examples. A multi-layered regulatory framework for AI must include a strong anti-bias layer starting from ex ante requirements on developers (diverse training data, bias mitigation techniques, transparency reports) to ex post accountability (audits, the ability to contest decisions, legal liability for discriminatory outcomes).[28] To ensure AI promotes equity rather than undermining it, protecting the rights and dignity of all communities.

4. Privacy and Data Protection

AI's hunger for data as its staple food and its capacity to infer sensitive information raises significant privacy concerns. Issues of privacy intersect with AI in multiple ways from the collection of personal data to train AI models, the possibility of AI-driven surveillance, and automated decision-making that affects individuals' information autonomy. Each jurisdiction's data protection landscape influences how AI is regulated:

European Union:

One of the strongest privacy regimes in the world is reflected through the General Data Protection Regulation (GDPR). GDPR, which took effect in 2018, imposes strict requirements on processing personal data and includes principles of consent, purpose limitation, data minimization, and rights for individuals over their data. These principles are the groundwork for the protection of rights of the victim. Critically, GDPR directly addresses automated decision-making in Article 22, granting individuals the right not to be subject to decisions based solely on automated processing that have significant effects, unless certain safeguards are in place.[29] This provision essentially means that if, for example, an AI system was to algorithmically approve or deny loans or filter job applications, EU residents have a right to request human intervention or an explanation. The logic is to prevent "black box" algorithms from having unchecked

[26] Digital Personal Data Protection Act, 2023, ss 4, 12.

[27] Ministry of Electronics & IT, India AI Governance Guidelines 2025.

[28] NITI Aayog, Principles for Responsible AI (2021); Regulation (EU) 2024/1689, arts 10, 61.

[29] Regulation (EU) 2016/679, art 22.

power over individuals' lives thereby a reflection of European values that prioritize privacy and dignity over purely efficiency gains. In addition, GDPR's requirements on transparency (Articles 13–15) mean organizations deploying AI must inform people that AI is involved and, upon request, provide information about how need of processing exists which pushes AI developers towards more interpretable models.[30] With the advent of the AI Act, the EU is supplementing data protection law with AI-specific rules. The AI Act and GDPR are designed to work parallelly as the AI Act governs the design and deployment of AI systems (e.g. requiring risk assessments, documentation, and conformity assessments for high-risk AI), while the GDPR continues to protect how those AI systems handle personal data. For instance, an AI recruiting tool in the EU must both comply with the AI Act (if high-risk, ensure oversight, accuracy, etc.) and respect GDPR (e.g. not use personal data beyond stated purposes, avoid processing sensitive data like race unless exceptions apply, etc.). The EU is also updating other laws, such as the Digital Services Act and Data Act, to regulate data use in algorithms and promote data sharing in privacy-preserving ways.[31] There are few cases where the AI use pose grave privacy threats and are banned or curtailed under the AI Act. Such as the real-time biometric identification in public spaces (like live facial recognition by police) is generally prohibited due to its intrusiveness. This comprehensive approach positions the EU as a leader in "privacy by design" for AI: future. The AI systems in Europe are expected to have privacy and transparency features built-in, and violations could lead to hefty fines (under GDPR or the AI Act's penalty provisions).[32] The underlying principle is clear: privacy is a fundamental right in the EU, so AI innovation must respect individuals' control over their data and identity. This is a key layer of the multi-layered framework where the robust data protection is non-negotiable, ensuring that any advancements in AI shall not come at the cost of personal privacy.

United States:

The U.S. lacks a single comprehensive data privacy law at the federal level, which means AI-related privacy protections are uneven. Instead, there is a patchwork of sectoral laws (like HIPAA for health data, FERPA for educational records, and COPPA for children's online data)[33] and some state laws (California's CCPA/CPRA giving importance to consumer rights over their personal information).[34] With no national framework large swathes of personal data remain either unregulated or under-regulated. For example, data collected from social media or public sources can be used to train algorithms with relatively few restrictions, if general consumer protection laws aren't violated. There are growing efforts to address AI and privacy. Federal agencies like the FTC have asserted they will go after companies if the use of personal data in AI algorithms is deceptive or causes harm (the FTC has warned against "snake oil" AI claims and inadequate data security). And privacy concerns have been a driving force in calls for AI regulation and can be implied through a privacy backlash in the U.S., leading to bans or moratoria by cities and even federal agencies (e.g. a temporary federal ban on police use of Clearview AI's face database, and the Defense Department's internal restrictions). In 2023, the Biden Administration issued Executive Orders on AI that include directives to protect privacy, such as developing standards for privacy-preserving AI (like techniques to train AI on encrypted data or synthetic data). There is also dual-party interest in a national data privacy law, which would indirectly constrain AI, but that is still pending. There have been some recent proposals like the Algorithmic Accountability Act which includes requirements for data protection impact assessments for AI systems, recognizing that flawed data practices (e.g. scraping personal data without consent, using biased or outdated data) are at the root of many AI issues. The ACLU and others highlighted the problem of AI systems relying on massive personal datasets collected without individuals' knowledge, and call the need for greater transparency and consent for AI data use Models like ChatGPT are trained on huge internet text corpora, raising questions about the privacy of content and with issues involved like copyright, patent etc., As soon as GDPR came into force, Italy briefly banned ChatGPT until it implemented

[30] Regulation (EU) 2016/679, arts 13-15.
[31] Regulation (EU) 2022/2065 (DSA); Regulation (EU) 2023/2854 (Data Act).
[32] Regulation (EU) 2024/1689, arts 5, 71; Regulation (EU) 2016/679, art 83.
[33] Health Insurance Portability and Accountability Act, 42 U.S.C. §§ 1320d et seq.; Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
[34] Cal. Civ. Code §§ 1798.100-1798.199 (CCPA/CPRA); Cal. Privacy Protection Agency, Automated Decision-Making Technology Regulations (2025).

GDPR measures and there is no equivalent measure in U.S. The U.S. approach to privacy in AI is currently more reactive and industry-driven where the companies are publishing AI ethics policies promising privacy. The tech firms are investing in various forms of privacy and other states (like California, Virginia, etc.) enforce baseline privacy rights that apply to AI uses of personal data. A multi-layered governance framework in the U.S. context would likely entail layering new AI-specific transparency and consent requirements atop the existing consumer privacy rights. For instance, requiring companies to disclose if consumer data will be used for AI model training, giving individuals an opt-out or compensation, and ensuring algorithms are audited for unwarranted intrusions (like inferring sensitive traits). India has recently made significant strides by enacting the Digital Personal Data Protection Act, 2023 (DPDP Act) replacing an earlier draft Personal Data Protection Bill.[35] It establishes a foundational privacy framework laying down essential requirements such as consent required for using personal data, mandates data security measures, provides for data subject rights (like correction and grievance redress), and creates a Data Protection Board for enforcement. For example, if an Indian company uses an AI system that profiles individuals for lending or hiring, the personal data input and output are covered by the DPDP Act (ensuring, for instance, that only necessary data is collected, and individuals can seek correction of erroneous data). DPDP Act "lacks AI-specific provisions" as it does not explicitly address automated decision-making or the requirement of algorithmic transparency and additional rules or guidelines are needed to tackle uniquely AI-driven privacy issues. Re-identification from anonymized data infringes the privacy of individuals who never consented but whose data might be scraped online for AI training, and the use of AI by the state for surveillance. On the latter, India has seen rapid adoption of facial recognition systems for policing and administration without a comprehensive surveillance law which has raised alarm amongst people. The Supreme Court of India's judgment in K.S. Puttaswamy vs Union of India (2017) recognized privacy as a fundamental right, which implies that any AI-enabled infringement (like intrusive surveillance or indiscriminate data processing) could be constitutionally challenged.[36] Yet, without clear statutes or regulations, it's difficult to define the limits. The government's India AI Guidelines 2025 acknowledge these concerns and call for incorporating principles of privacy, security, and transparency by design in AI systems.[37] There is need for privacy-preserving techniques like anonymization, encryption, federated learning to be part of AI development. Reserve Bank's guidelines on digital lending require that automated decisions be made transparent and consumer data should not be misused for training.[38] A multi-layered AI framework in India would likely involve amendments or rules under the DPDP Act focusing on AI, such as a right to explanation for significant AI decisions (akin to GDPR's Article 22).[39] The requirements for Data Protection Impact Assessments taken when deploying high-risk AI is to evaluate privacy and security risks. Strict oversight compliance on government AI projects that handle personal data to ensure proportional use and data minimization in, say, law enforcement AI. India might consider restrictions on particularly privacy-invasive AI uses for example, regulating AI-driven biometric surveillance or deepfake technology. The Constitution's emphasis on personal liberty combined with the new DPDP Act framework provides a strong basis to build these AI-specific privacy protections. In conclusion, privacy and data protection form a vital layer of AI governance.

The EU's model demonstrates how protecting personal data and giving individuals rights over automated decisions can foster trust in AI systems and prevent abuses. The U.S., while currently more fragmented, is moving towards recognizing privacy as essential for AI's sustainable growth. A multi-layered framework would ensure any AI system, whether developed in Silicon Valley, Bengaluru, or anywhere else, adheres to common principles of privacy such as to collect and use personal data lawfully and minimally, be transparent about automated processing, allow individuals control and recourse, and impose strict accountability for misuse. This not only protects individual rights but also aligns with global trends,

[35] India. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

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

[37] Ministry of Electronics and Information Technology. India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation. New Delhi: Government of India, 2025.

[38] Reserve Bank of India. Reserve Bank of India (Digital Lending) Directions, 2025, paras 12-15.

[39] India. Digital Personal Data Protection Act, 2023, ss 6-7.

facilitating cross-border data flows and AI innovation in a rights-respecting manner.

Use of AI in the Judicial System

The deployment of AI in judicial or quasi-judicial processes such as court decision support, sentencing recommendations, predictive policing, and legal research raises distinct concerns at the intersection of technology and the rule of law. The question here is how (and whether) to integrate AI into functions traditionally performed by judges, lawyers, or law enforcement, and what kind of safeguards are needed to preserve fair trial rights, due process, and judicial accountability. The EU, US, and India are each cautiously exploring this frontier:

European Union:

In the EU, the idea of "AI judges" or fully automated judicial decisions is generally approached with great caution. The EU AI Act classifies any AI system intended to assist in "administration of justice" as high-risk, meaning such systems must meet stringent requirements before they can be used whether used to suggest sentences, predict case outcomes, or filter legal documents. The high-risk designation triggers obligations on providers by ensuring that the system must be trained on high-quality (unbiased) data, is transparent, and subject to human oversight always. Moreover, one of the AI Act's prohibited practices (Article 5) is the use of AI for social scoring by public authorities, which reflects a broader principle that core public sector decisions affecting the rights should not be left to opaque algorithms.[40] While social scoring is not the same as court decisions, the ban hints discomfort with algorithmic assessment of citizens' worthiness or risk in a way that could be a "notch" for defendants. Commission for the Efficiency of Justice (CEPEJ) in 2018 adopted the European Ethical Charter on the use of AI in judicial systems.[41] This charter sets principles like respecting fundamental rights, ensuring the quality and security of data, transparency, impartiality, and "AI should not undermine the ultimate authority and autonomy of human judges. For example, if an AI tool provides a sentencing suggestion, the judge must remain free (and obliged) to disagree if necessary, and the AI's reasoning should be explainable. The EU's overall stance is that AI can assist in judicial tasks (like sorting cases, legal research, translations, or even suggesting outcomes based on precedent), but it should never replace the human judgment required in applying the law. The right to a fair trial under the European Convention on Human Rights implies a right to an impartial human judge and delegating that role to a machine, especially a non- transparent one, could violate that right. Even for simpler tasks, European data protection authorities have warned against fully automated decision-making in law enforcement or justice.

In sum, Europe's multi-layered framework treats "AI in justice" as a sensitive layer that must be tightly controlled. Any adoption of AI by courts should be accompanied by measures like pilot testing, independent auditing, disclosure to parties and possibilities to challenge any AI-influenced decision. For instance, courts in Estonia have tested an online dispute resolution system for small claims that uses algorithms, but with human review.

United States:

The U.S. had some of the earliest and most high-profile forays into algorithmic tools in the justice system, sparking significant debate. In criminal justice, predictive policing algorithms are used by some police departments to allocate resources to locations deemed high risk for crime and has been criticized to reinforce biased policing patterns. Risk assessment algorithms like COMPAS have been used by judges or parole boards in many states to help determine bail, sentencing, or parole decisions by scoring defendants on their risk of reoffending. The use of COMPAS led to a landmark case, State v. Loomis (Wisconsin, 2016),[42] where a defendant challenged a sentence influenced by a secret algorithm. The court allowed COMPAS's use but required warnings about its limitations. The broader fallout was that ProPublica's investigative report found COMPAS was biased against Black defendants, as mentioned, falsely flagging them high-risk

[40] Regulation (EU) 2024/1689, art 5(1)(c).

[41] European Commission, Proposal for a Directive on adapting non-contractual civil liability rules to AI COM(2022) 496 final (withdrawn 2025).

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

at roughly twice the rate of white defendants. This revelation fueled a national discussion on the due process and bias implications of using AI in courts. Concerns include defendants' right to examine and challenge evidence (if an algorithm's workings are proprietary, how can one cross-examine it?), the risk of automating racial bias, and the possibility of judges placing undue trust in a seemingly objective "score" (often called automation bias). As a result, some jurisdictions pulled back – for example, California passed a law in 2018 to end the use of risk assessment tools in pre-trial decisions until they could be better vetted. On the civil side, AI hasn't yet taken a direct role in adjudication, but there are startups offering AI judging for online dispute resolution in minor cases, and AI is heavily used in legal research (e.g. tools that predict case outcomes or assist in drafting). The U.S. being a common-law system also means AI could influence the development of law – e.g. if an AI tool predicts damages in civil cases and becomes widely used, it might create de facto standards. So far, there is no federal regulation specific to AI in the judiciary, but the National Center for State Courts and other bodies have issued guidelines. Many emphasize transparency, validation, and voluntary use. One key principle resonating in U.S. discourse is that AI should not be the final decision-maker in any court action – it can provide input, but a human official must make the ultimate decision, preserving human accountability. Also, any risk assessment used should be statistically validated for accuracy and fairness in that jurisdiction's population. An important development in late 2023 was the Bipartisan Policy Center's task force report on AI in Justice, which recommended standards and possibly a certification system for algorithms used by courts or law enforcement.[43]

Meanwhile, the DOJ's Civil Rights Division and the Department of Homeland Security have been investigating algorithmic tools (like "extremism" screening algorithms) for potential bias.[44] The upshot is that the U.S. approach is still evolving, driven by a mix of court rulings, advocacy, and local policy. It exemplifies both the promise of AI (efficiency, consistency) and the peril (bias, opacity) in the justice context. A multi-layered governance approach in the U.S. might involve: establishing federal guidelines or oversight for any AI used in criminal justice (to ensure constitutional rights are safeguarded), promoting best practices like algorithmic transparency and independent audits, and empowering defendants with rights to challenge algorithmic evidence. Notably, the ACLU and other groups have litigated to get access to algorithmic formulas (with mixed success). Furthermore, some U.S. states are considering legislation to ban outright the use of certain AI in sentencing or policing until fairness can be assured. These cautionary moves align with the idea that the rule of law must not be compromised by unaccountable technology.

India:

India's judiciary and legal system, burdened by massive backlogs of cases, have shown interest in AI primarily as a tool to increase efficiency. The Supreme Court of India launched an AI-driven portal called SUPACE (Supreme Court Portal for Assistance in Court Efficiency) in 2021, aimed at helping judges with legal research by quickly providing relevant facts and precedents for cases. Importantly, the then-Chief Justice S.A. Bobde explicitly stated that SUPACE would not venture into judicial decision-making – its role is limited to data processing and aiding judges, not deciding cases.[45] This reflects a deliberate stance: even as the judiciary experiments with AI to manage workload, it is wary of ceding any decision- making power to algorithms. Indian jurists recognize the potential pitfalls: bias is a top concern, as any AI system used in courts might carry the prejudices present in its training data (e.g. past judgments or police records). Additionally, lack of transparency in AI could clash with the need for reasoned judicial orders – every court decision in India must articulate reasons, and if an AI influenced a decision, how would that be explained? The Centre for Law & Policy Research (CLPR) in India observed that even seemingly benign AI assistance can have "damaging consequences" if not checked, because it might subtly bias what information a judge sees first. For example, if an AI tool unthinkingly highlights past cases that led to acquittals more often than convictions (or vice versa), it might prime a judge's mind. The CLPR also cited the COMPAS example from the U.S. as a cautionary tale and echoed experts like Dr. Dory Reiling (of the EU) that external audits and explainability are needed for any AI in justice. As of now, India does not use AI for tasks like sentencing or

[43] Bipartisan House Task Force on AI, Report on Artificial Intelligence (2024).

[44] U.S. Dep't of Justice, Civil Rights Div., Examination of Allegheny Family Screening Tool (2023).

[45] Ajoy. "Artificial Intelligence and the Courts." Clpr.org.in, 2021. https://clpr.org.in/blog/artificial-intelligence-and-the-courts/.

bail decisions; these remain purely human decisions, and there's a general consensus that it should stay that way for the foreseeable future. Instead, the focus is on augmenting human judges – for instance, using AI for translating judgments into regional languages (the Supreme Court's SUVAS translation system),[46] or summarizing lengthy case files (the intended use of SUPACE). On the policing side, however, some Indian states have shown interest in predictive policing tools (as mentioned with Delhi's CMAPS), and facial recognition is being rolled out in airports and city surveillance.

These raise judicial use issues indirectly – e.g., if police decisions influenced by AI lead to arrests, those cases come to court possibly tainted by algorithmic bias. The judiciary might then have to deal with evidence or procedures that involve AI (was a defendant flagged by an AI as high risk, leading to heavier bail terms?). No clear protocols exist yet for these scenarios. Looking ahead, the NITI Aayog (a government think tank) and the Ministry of Electronics & IT have advocated for using AI in legal analytics and court administration, but with strong ethical guidelines.[47] A vision often discussed is AI handling mundane procedural matters to free up judges for core judicial work, but always under a judge's supervision. Therefore, aligning with a multi-layered regulatory ethos, India would need to craft guidelines or rules that codify the limits and requirements for AI in judicial contexts. This could take the form of: Supreme Court or High Court rules on the use of AI tools in courts (perhaps requiring certification of any such tool for accuracy and bias, disclosure to litigants if used, and an option to override), and legislation or policy for law enforcement use of AI (ensuring any predictive policing or forensic AI respects rights and can be challenged in court). India's constitutional framework – which guarantees the right to a fair trial and equality before law – implies that if AI is to be used, it must enhance, not diminish, those rights. Encouragingly, the discourse in India, much like Europe, emphasizes learning from other systems and proceeding carefully. The CLPR aptly concluded that any integration of AI into the justice system "must be done with care and deep engagement with potential pitfalls and unintended consequences," and that India "must closely look at and learn from the experience of other judicial systems that've adopted AI." That sentiment captures the essence of a layered approach – build on best practices, ensure human control at every step, and be vigilant through oversight mechanisms.

In summary, AI in the judicial system is a frontier that requires balancing efficiency gains with core legal values. The European approach provides a principled framework: classify such uses as high-risk and enforce human-centric requirements. The American experience provides cautionary lessons on what happens if bias and transparency aren't addressed up front. India's early stance underscores the importance of gradual, controlled adoption with judges firmly in charge. A multi-layered governance framework for this domain might include ethical charters, legal rules, and technical standards working in harmony. For instance, an ethical charter (like CEPEJ's) sets broad principles, legal rules (in legislation or court practice directions) set binding limits (e.g., "no purely algorithmic decisions in adjudication"), and technical standards ensure AI systems meet reliability and fairness benchmarks. Ultimately, judicial use of AI must uphold the rule of law – meaning that the introduction of any AI should not compromise fairness, equality, or the public's trust in the justice system's integrity.

Conclusion

Across the European Union, United States, and India, the drive to regulate AI is motivated by a common realization: AI technologies, if left unguided, can both revolutionize and destabilize society. The comparative analysis of liability, bias, privacy, and judicial use of AI reveals that while each jurisdiction's approach is shaped by its legal culture and policy priorities, there is a clear convergence towards a multi-layered framework that marries innovation with fundamental rights and social accountability. From the EU's risk-based AI Act, we learn the value of a graded regulatory structure – one that imposes proportionate controls based on an AI system's potential to cause harm. This layered approach ensures that the most dangerous AI practices are flatly prohibited or heavily constrained, moderate-risk applications are made transparent and fair, and low-risk uses can flourish under voluntary codes. The EU's example demonstrates

[46] Supreme Court of India, SUVAS: Supreme Court Vidhik Anuvaad Software (2021 onwards).

[47] NITI Aayog, Principles for Responsible AI (2021).

that comprehensiveness and clarity in AI governance are achievable, and indeed can coexist with tech innovation (by establishing clear "rules of the road" that encourage trust in AI). The multi-layered regulatory framework proposed in this paper echoes that model: it envisions a combination of hard law, soft law, and ethical principles, each reinforcing the other. For instance, hard laws (statutes, regulations) can set minimum standards and liability rules; soft laws (guidelines, industry standards) can fill technical gaps and adapt quickly to new developments; and ethical principles (like fairness, accountability, transparency – often dubbed the FAT principles of AI) provide the normative compass ensuring that human and social values remain at the core. The U.S. and Indian perspectives add crucial dimensions to this framework. The U.S. brings to the table a rich tapestry of sectoral insights and grassroots innovation – its experience shows that one-size- fits-all may not work for AI, say, in medicine versus transportation, and that empowering domain- specific agencies (FDA, DOT, etc.) to issue tailored AI guidance can be effective. It also highlights the role of civil society and local governments in pushing the envelope on issues like algorithmic bias and surveillance, which can then percolate up to national policy. Any robust AI governance framework should thus be multi-layered not only in rules but in stakeholders: involving technologists, regulators, affected communities, and domain experts in an iterative policy-making process. Meanwhile, India's situation underscores the importance of grounding AI regulation in constitutional values and social context. India's call for a rights-based AI framework is a reminder that technology should serve humanity and justice, not the other way around. When crafting AI laws, considerations of equity (e.g. preventing AI from widening social gaps), accountability (e.g. clarifying who answers for AI-caused harm), and inclusive growth (leveraging AI for social good) must be interwoven. In practice, this could mean adopting affirmative obligations like algorithmic impact assessments focusing on impacts to disadvantaged groups, or creating public-sector AI literacy programs so that judges, policymakers, and citizens alike understand the tools being deployed around them. A key takeaway from all three jurisdictions is the necessity of algorithmic accountability – mechanisms to ensure AI systems can be audited, explained, and corrected. Whether it's a biased loan algorithm or a flawed police predictive model, transparency and accountability are paramount to detect issues and uphold individuals' rights. The frameworks developing worldwide increasingly incorporate this: the EU will require logging of AI system operations and accessibility for regulators; the US is seeing a rise of algorithmic audit requirements; India's thinkers propose rights to explanation and appeal. Ensuring that our multi-layered regulatory framework embeds accountability at every level (from developers certifying their systems, to government oversight bodies with audit powers, to courts accessible for redress) is crucial. As a noted expert quipped, "accountability cannot exist without transparency", and thus our governance model must mandate transparency as the foundational layer.

In aligning the approaches of the EU, US, and India, this paper demonstrates that there is a path forward to a coherent and just AI governance regime. Such a regime would feature:

1. Clear liability rules so that those harmed by AI have recourse and those deploying AI take proactive safety measures 5 (learning from EU's proposals and US/India's current gaps).

2. Robust anti-bias and fairness mandates to ensure AI systems promote social justice rather than undermine it (building on EU's fundamental rights approach, US civil rights enforcement, and India's constitutional vision).

3. Strong privacy and data protection controls as a bulwark against intrusive and illegitimate data uses (combining EU's GDPR ethos, evolving US state laws, and India's new DPDP framework).

4. Strict oversight of AI in public functions like the judiciary or policing, preserving human accountability and the rule of law (inspired by Europe's human-in-command principle, US cautionary experiences, and India's careful experimentation). These layers are not silos; they interconnect. For example, bias mitigation is tied to data quality (privacy layer) and to who is liable if discrimination occurs (liability layer).

A multi-layered framework recognizes these interdependencies and fosters coordination – for instance, a Data Protection Authority working with an AI Ethics Board and sectoral regulators to jointly review a high-risk AI system before it hits the market. Finally, it is worth noting that AI regulation is not a one-and-done effort. Technology evolves, and laws must adapt. The approaches surveyed here are all subject to ongoing refinement – the EU AI Act will undergo amendments and delegated acts, U.S. agencies will continue issuing guidance, and India will likely update its policies as it learns from initial implementations. International cooperation will also be a layer of growing importance, as AI is a global phenomenon. The alignment of EU, US, and India on core principles could pave the way for international standards or treaties (as hinted by the Council of Europe's draft convention) that ensure AI developers cannot evade regulations by moving to more lenient jurisdictions. In essence, a multi-layered framework is also a multi-level one: local, national, and international levels all have roles to play. In conclusion, by examining and aligning these three jurisdictions' approaches, this paper underscores that effective AI governance requires a synchronized, multi-faceted strategy – one that holds algorithms to the highest standards of accountability, fairness, and respect for human values. Such an approach not only addresses the immediate concerns of liability, bias, privacy, and judicial integrity, but also builds the foundation for sustainable and socially beneficial AI innovation. In the words of the ACLU's Deborah Archer, "it is not enough to have diverse people in the room; we must also ensure those people have the power, resources, and rights to shape AI's impact". A multi-layered regulatory framework, anchored in comparative insights and social justice, is ultimately about empowering people and their institutions to steer AI – so that this transformative technology truly serves the public good in the European Union, the United States, India, and beyond.

References

1. ACLU Policy Brief, Artificial Intelligence and Racial Injustice (2024).
2. ACLU, Accountability in Artificial Intelligence (2025).
3. Ajoy. "Artificial Intelligence and the Courts." Clpr.org.in, 2021.
4. American Civil Liberties Union. "AI Could Exacerbate Inequality, Experts Warn." Aclu.org, 22 July 2025.
5. Bipartisan House Task Force on AI, Report on Artificial Intelligence (2024).
6. Cal. Civ. Code §§ 1798.100-1798.199 (CCPA/CPRA); Cal. Privacy Protection Agency, Automated Decision-Making Technology Regulations (2025).
7. Canca, N. C., and E. Quintais. "Human Oversight Requirements for AI Decision-Making." Computer Law & Security Review 49 (2023).
8. DLA Piper. "Fairness / Unlawful Bias in the European Union." Intelligence.dlapiper.com, 2025.
9. European Commission, Proposal for a Directive on adapting non-contractual civil liability rules to AI COM(2022) 496 final (withdrawn 2025).
10. European Parliamentary Research Service. Artificial Intelligence and Liability for the Purposes of Civil Liability. Brussels: European Parliament, 2023.
11. Government of Iceland. "Joint Nordic Statement: Artificial Intelligence and the Global Dialogue on AI Governance." Government.is, 19 February 2025.
12. Health Insurance Portability and Accountability Act, 42 U.S.C. §§ 1320d et seq.; Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
13. India. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
14. India. Digital Personal Data Protection Act, 2023, ss 6-7.
15. K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
16. Legacy Law Offices. "AI on Trial: Rethinking Liability in India's Current Legal Framework." Legacylawoffices.com, 9 September 2025. https://www.legacylawoffices.com/ai-on-trial-rethinking-liability-in-indias-current-legal-framework/.
17. Ministry,of Electronics and Information Technology. India AI Governance Guidelines: Enabling Safe

and Trusted AI Innovation. New Delhi: Government of India, 2025.

18. Ministry of Electronics and Information Technology. India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation. New Delhi: Government of India, 2025.

19. NITI Aayog, Principles for Responsible AI (2021).

20. Norton Rose Fulbright. “Artificial Intelligence and Liability.” Nortonrosefulbright.com, 2025.

21. Norton Rose Fulbright. “Artificial Intelligence and Liability.” Nortonrosefulbright.com, 2024.

22. Pandey, Swaraj. “Regulation of Artificial Intelligence in India: Legal Challenges and Policy Recommendations.” SSRN Electronic Journal, 2025.

23. RAND Corporation. Developing Effective Governance for Synthetic Data and Generative AI Systems. Santa Monica, CA: RAND, 2025. https://www.rand.org/pubs/research_reports/RRA3243-3.html.

24. RAND Corporation. Developing Effective Governance for Synthetic Data and Generative AI Systems. Santa Monica, CA: RAND Corporation, 2025.

25. Regulation (EU) 2016/679 (GDPR), art 22.

26. Regulation (EU) 2016/679, art 22.

27. Regulation (EU) 2016/679, arts 13-15.

28. Regulation (EU) 2022/2065 (DSA); Regulation (EU) 2023/2854 (Data Act).

29. Regulation (EU) 2024/1689, art 10(2)(f), (5).

30. Regulation (EU) 2024/1689, art 5(1)(c).

31. Regulation (EU) 2024/1689, arts 5, 71; Regulation (EU) 2016/679, art 83.

32. Řeserve Bank of India. Reserve Bank of India (Digital Lending) Directions, 2025, paras 12-15.

33. State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

34. Supreme Court of India, SUVAS: Supreme Court Vidhik Anuvaad Software (2021 onwards).

35. Tiwari, Shreya. “Towards Rights-Based AI Framework In India: Bridging Global Models And Constitutional Duties.” Livelaw.in, 26 July 2025.

36. Tiwari, Shreya. “Towards Rights-Based AI Framework In India: Bridging Global Models And Constitutional Duties.” Livelaw.in, 26 July 2025.

37. U.S. Dep't of Justice, Civil Rights Div., Examination of Allegheny Family Screening Tool (2023).

38. Vidhi Centre for Legal Policy, "India's Tryst With Predictive Policing" (2021).

39. White House Office of Science and Technology Policy, Blueprint for an AI Bill of Rights (2022).

40. White House Office of Science and Technology Policy, Blueprint for an AI Bill of Rights (2022).

41. White House OSTP, Blueprint for an AI Bill of Rights (Oct. 3, 2022).