INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

A STUDY ON PUBLIC OPINION REGARDING THE LEGAL CHALLENGES AND IMPLICATIONS OF ARTIFICIAL INTELLIGENCE REGULATION: A COMPARATIVE GLOBAL PERSPECTIVE.

AUTHORED BY - *NUSRATH M S & **MAHALAKSHMI M. K

ABSTRACT

The global surge in the deployment of Artificial Intelligence (AI) across sectors—ranging from criminal justice and healthcare to finance and governance—has significantly outpaced the evolution of legal frameworks capable of addressing its multifaceted implications. This research undertakes a doctrinal and empirical study of public opinion concerning legal challenges posed by AI, focusing on five core issues: legal liability, algorithmic bias, data privacy, criminal justice, and labour displacement. Using a mixed-methods approach, this study captures the attitudes and concerns of the general public and compares them against prevailing legal doctrines and regulatory models from India, the European Union, the United States, and China. Public responses overwhelmingly support shared responsibility for AI-related harms, ethical oversight to combat bias, stronger data protection laws, transparency in predictive policing, and fair transitions in AI-augmented labour markets. The findings reflect a growing consensus that human rights, fairness, and democratic accountability must form the cornerstone of any legal response to AI. This study contributes to the global discourse by proposing a harmonized, rights-based, and participatory legal framework that is responsive to both technological innovation and societal expectations.

Key Words: *Artificial Intelligence Regulation – Algorithmic Bias – Legal Liability – Data Privacy – Comparative Legal Frameworks.*

*Under Graduate Student, B.COM LL. B (HONS.)., Email: shifananusrath0@gmail.com
**Assistant Professor, Email: mahalaksh9999@gmail.com
Dr. M. G. R. Educational and Research Institute Deemed to be University, Chennai, Tamil Nadu, India.

 ISSN: 2582-6433

INTRODUCTION:

Artificial Intelligence (AI) has transitioned from a niche domain of computer science to a transformative force across legal, economic, and social landscapes. Its applications span critical sectors such as healthcare, criminal justice, employment, finance, and public administration. As AI systems gain autonomy and complexity, they are increasingly making decisions that have significant consequences for human rights, civil liberties, and social justice. The unprecedented scale and opacity of AI decision-making raise pressing legal questions about responsibility, transparency, and fairness.

One of the most urgent challenges is the attribution of legal liability in the event of AI-induced harm. Traditional legal frameworks presuppose human agency and intent, yet AI operates through complex algorithms that may evolve unpredictably over time. For instance, if an autonomous vehicle malfunctions and causes a fatal accident, determining whether the developer, user, or manufacturer should be held liable becomes legally intricate. This dilemma is compounded by the "black box" nature of AI systems, where the rationale behind a decision often remains opaque—even to the engineers who designed it.

Case laws are beginning to confront such complexities. In United States v. Microsoft Corp. (2001), although not an AI case, the court held developers accountable for monopolistic system behaviors embedded in software, signaling potential parallels for AI responsibility. Similarly, in Donoghue v. Stevenson (1932), the principle of manufacturer liability laid the groundwork for contemporary debates on defective AI products. These foundational doctrines are now being stretched to accommodate entities that neither possess consciousness nor intention, yet act in legally consequential ways.

Furthermore, the risk of algorithmic discrimination has brought equality jurisprudence under strain. The Indian Supreme Court's decision in Navtej Singh Johar v. Union of India (2018) expanded constitutional protections to non-discriminatory digital practices, thereby providing a doctrinal basis for contesting AI bias under Articles 14 and 15. Likewise, People v. Loomis (2016) in the United States highlighted due process concerns when AI-driven risk assessments were used in criminal sentencing without allowing the defendant to challenge the system's logic.

Despite these developments, India's regulatory landscape remains underdeveloped. While the

 ISSN: 2582-6433

enactment of the Digital Personal Data Protection Act, 2023 has introduced basic data safeguards, there is still no comprehensive legislative framework addressing AI's legal and ethical ramifications. By contrast, the European Union has advanced the draft AI Act, which proposes a risk-tiered model of regulation, including outright bans on systems that pose "unacceptable risk" to fundamental rights.

This research is premised on the belief that public opinion—often overlooked in legislative discourse—should play a central role in shaping AI regulation. Empirical data drawn from this study suggests that citizens overwhelmingly demand shared responsibility for AI decisions, robust oversight to prevent bias, and enforceable rights against opaque algorithmic decisions. These findings highlight a critical normative gap between legal principles and social expectations.

In this context, the present study adopts a comparative and interdisciplinary approach, integrating doctrinal legal research, empirical public surveys, and cross-jurisdictional analysis. It aims to offer a framework for AI governance that is grounded in constitutional values, guided by public reasoning, and informed by global best practices.

OBJECTIVES OF THE STUDY:

This research aims to critically assess public opinion surrounding the regulation of Artificial Intelligence (AI) and analyse the legal implications of algorithmic systems from a global comparative lens. The key objectives are:

1. To investigate how the public perceives AI-related legal challenges in areas such as liability, bias, data privacy, criminal justice, and labour automation.
2. To identify gaps between technological advancement and existing legal frameworks, particularly in India.
3. To assess whether public opinion supports shared liability frameworks and ethical oversight mechanisms.
4. To compare the legal and policy approaches of India, the European Union, the United States, and China in addressing AI governance.
5. To propose inclusive, rights-based regulatory models rooted in constitutional values and public consensus.

 ISSN: 2582-6433

RESEARCH METHODOLOGY:

1. Study Design

   A mixed-methods design combining doctrinal legal research and empirical public survey analysis was adopted. This design enables both normative legal inquiry and data-driven insights.

2. Study Period and Setting

   The study was conducted over a three-month period between February 2025 and April 2025, during which both doctrinal research and empirical data collection took place. The research setting encompassed digital platforms to facilitate wide and accessible participation from individuals familiar with technological and legal developments. Given the interdisciplinary nature of the topic, the study focused on urban respondents across India, particularly those engaged in law, policy, technology, and related academic disciplines. The online environment allowed for efficient dissemination of the survey instrument, ensuring diversity in demographic representation while maintaining consistency in data collection procedures.

3. Target Population

   The sample included students, legal professionals, researchers, and working professionals aged 18 to 45 with baseline digital literacy.

4. Sampling & Respondent Criteria

   A total of 37 valid responses were gathered through structured questionnaires. Participants were required to have some awareness of digital technologies and legal systems.

5. Data Collection Methods

   Quantitative data was collected through multiple-choice questions framed around AI-related legal issues (e.g., liability, bias, privacy). Qualitative insights were collected through open-ended responses and cross-referenced with doctrinal legal research.

6. Data Analysis

   Statistical analysis was performed using frequency distribution and percentage representation. Findings were then mapped against normative legal standards and comparative international laws.

7. Trustworthiness and Reliability

   Survey questions were pre-tested for clarity. Anonymity and voluntary participation were ensured. Legal frameworks and case laws were sourced from primary legislation, official court records, and scholarly databases.

 ISSN: 2582-6433

8. Ethical Consideration

   No personally identifiable information was collected. Participation was entirely voluntary, and informed consent was implied through response submission.

DATA ANALYSIS AND FINDINGS

This section presents the empirical insights drawn from a structured survey conducted to understand public perceptions on the legal and ethical dimensions of Artificial Intelligence (AI) regulation. A total of 37 valid responses were analysed using simple statistical tools. Each table below corresponds to a specific theme of the study and is followed by a brief interpretation.

Table 1: Public Opinion on Legal Responsibility in AI – Induced Harms

Legal Actor Preferred for Responsibility	Number of Responses	Percentage (%)
Shared Responsibility (Developers, Users, Manufacturers)	18	48.65%
Developers Only	15	40.54%
AI System as Legal Person	2	5.41%
Users Only	1	2.7%
Others	1	2.7%

Interpretation: A majority support a shared liability model, reinforcing the need for multi – stakeholder accountability in AI governance.

Table 2: Awareness of Algorithmic Bias

Response Option	Number of Responses	Percentage (%)
Yes, aware of algorithmic bias	24	64.86%
Not Sure	9	24.32%
No	4	10.81%

Interpretation: Over 60% acknowledge AI bias, underlining the importance of regulatory checks for fairness and inclusiveness.

 ISSN: 2582-6433

Table 3: Preferred Legal Response to AI Discrimination

Option Selected	Number of Responses	Percentage (%)
Independent Ethical Oversight	10	27.03%
Mandatory AI Impact Assessments	13	35.14%
Algorithmic Transparency Requirements	7	18.92%
Inclusive Training Data Mandates	5	13.51%
Others	2	5.4%

Interpretation: A strong - preferences exists for impact assessments and oversight bodies, showing public desire for proactive legal mechanisms.

Table 4: Public Preferences for Data Protection Measures

Data Privacy Tool or Right Supported	Number of Responses	Percentage (%)
Zero – Data AI Models	10	27.03%
Right to Be Forgotten	9	24.32%
Data Sovereignty Laws	7	18.92%
International Data Sharing Agreements	9	24.32%
None of the Above	2	5.4%

Interpretation: The Preference for Privacy – enhancing AI design and control over personal data demonstrates a growing rights – based data culture.

Table 5: Public Trust in AI for Criminal Justice Use

AI in Criminal Justice Should Be	Number of Responses	Percentage (%)
Used only under Human Oversight	24	64.86%

 ISSN: 2582-6433

Completely Trusted for Independent Decisions	5	13.51%
Not Used at All	8	21.62%

Interpretation: The public strongly supports human – AI collaboration in justice rather than full autonomy.

Table 6: Concerns about AI – Induced Job Displacement

Preferred Response to AI and Employment	Number of Responses	Percentage (%)
Retraining Programs	9	24.32%
AI – Human Collaboration Models	13	35.14%
Universal Basic Income	8	21.62%
Strict Restrictions on Automation	5	13.51%
No Regulation Needed	2	5.41%

Interpretation: Majority favour coexistence models over restrictive or fully autonomous employment models.

Table 7: Familiarity with India's Digital Personal Data Protection Act, 2023

Awareness Level of DPDPA 2023	Number of Responses	Percentage (%)
Aware and Understand the Basics	12	32.43%
Heard of It but Not Aware in Depth	15	40.54%
Not Aware at All	10	27.03%

Interpretation: There is still a gap in awareness about India's key digital law, which may weaken informed participation in AI policy debates.

 ISSN: 2582-6433

Table 8: Opinion on Need for a Separate AI Regulation in India

View on AI – Specific Law	Number of Responses	Percentage (%)
Yes, Urgently Needed	25	67.57%
Maybe, After More Discussion	8	21.62%
No, Existing Laws Are Sufficient	4	10.81%

Interpretation: Public sentiment favours immediate AI legislation, reflecting regulatory anxiety and proactive demand for legal clarity.

QUALITATIVE INSIGHTS

While quantitative data captures measurable trends, qualitative analysis unveils the reasoning, concerns, and expectations behind public opinion on AI regulation. Responses to open-ended questions revealed several recurring themes—concerns over rights, trust in legal systems, and the urgent need for ethical governance.

1. Trust and Transparency Are Paramount

   A recurring sentiment was the distrust in opaque AI systems, especially in sensitive domains like policing and finance. Respondents emphasized that AI must be explainable, auditable, and subjected to judicial scrutiny.

   "I fear AI will make decisions that no one can explain, and that's scary in a democracy."

   "There should be a right to question AI decisions just like we can challenge administrative actions in court."

   This aligns with global policy trends such as the EU's proposed right to explanation, reinforcing the demand for human oversight in algorithmic decision-making.

2. Shared Accountability Resonates with Public Reasoning

   Many respondents expressed discomfort with the idea of AI being solely blamed for harmful outcomes. Instead, they proposed shared accountability among developers, operators, and regulators.

   "You can't blame the machine—it does what it's told. The blame should lie with those who made it and use it."

   This insight supports the shared liability model that has been evolving in European and Canadian regulatory frameworks.

3. Ethical Bias and Discrimination Are Social Justice Concerns

 ISSN: 2582-6433

The qualitative data revealed a profound awareness of social implications, particularly AI's potential to reinforce caste, gender, and racial biases.

"How do we know if an AI is not biased against women or Dalits? Algorithms reflect society."

"Bias in data is real. We need oversight committees, like ethics boards for hospitals."

Respondents echoed concerns raised in cases such as State v. Loomis (USA), where predictive algorithms in criminal justice showed racial skew.

4. Concerns Over Data Control and Privacy

   Participants expressed alarm over mass data collection and the lack of user control in digital environments.

   "We give data without knowing how it is used. AI makes it worse."

   "There should be a way to delete our data forever. Right to be forgotten must be enforced."

   This directly aligns with the emerging privacy jurisprudence under Puttaswamy (2017) and demands for extending its logic to AI applications.

5. Suggestions for Public Participation

   Several participants felt excluded from the ongoing policy discourse and called for citizen engagement and consultation in AI law-making.

   "We the people should have a say in how AI is governed."

   "It should not just be tech companies and bureaucrats making the rules."

   This underscores the need for democratic accountability, similar to models adopted in Canada and deliberative assemblies proposed in the UK's AI governance discussions.

6. Demand for Education and Awareness

   Many responses highlighted a need for digital literacy and education on AI risks and rights.

   "Most people don't know what AI does. That needs to change before regulating it."

   "We must start teaching AI ethics and laws from school or college levels."

This view advocates for institutional reforms and public education to bridge the AI awareness gap.

These qualitative insights validate and deepen the statistical findings. The public does not passively accept AI's rise—they critically evaluate its impact and seek a regulatory system rooted in fairness, accountability, and human dignity.

 ISSN: 2582-6433

COMPARATIVE LEGAL APPROACHES TO AI REGULATION

As Artificial Intelligence continues to influence governance, industry, and civil liberties, regulatory responses vary across jurisdictions—reflecting differing legal cultures, policy priorities, and technological maturity. This section examines how key global regions—the European Union (EU), United States (US), China, and India—approach the legal governance of AI, with a focus on risk classification, liability, privacy, and public oversight.

1. European Union (EU): Risk-Based and Rights-Oriented Regulation

   The EU has been a global leader in AI governance, prioritizing human rights and ethical safeguards. The proposed Artificial Intelligence Act (2021) classifies AI systems into four risk categories:

   - Unacceptable risk: systems like social scoring are banned outright.
   - High-risk AI: including biometric identification and credit scoring—requires risk assessment, transparency, and human oversight.
   - Limited risk: requires disclosure that the system is AI-powered (e.g., chatbots).
   - Minimal risk: no intervention needed.

   The General Data Protection Regulation (GDPR) complements this by protecting personal data rights and establishing mechanisms like the right not to be subject to automated decision-making (Article 22).

   EU institutions also emphasize algorithmic explainability, human control, and auditability, making it the most comprehensive and rights-aligned framework globally.

2. United States (US): Sector-Specific and Innovation-Focused

   In contrast to the EU, the US favors market-driven regulation with industry-specific oversight. No unified AI law exists at the federal level, though regulatory bodies such as:

   - FDA oversee AI in healthcare
   - FTC addresses deceptive AI practices;
   - EEOC provides guidance on bias in AI hiring tools.

   Legislative proposals like the Algorithmic Accountability Act (2019, reintroduced in 2022) aim to establish risk audits for AI systems, but progress has been slow.

   Courts have intervened in isolated cases, such as People v. Loomis (2016), which questioned the due process implications of using risk-assessment algorithms in

 ISSN: 2582-6433

sentencing.

The US model prioritizes innovation and corporate autonomy, often at the cost of comprehensive public accountability.

3. China: State-Centric, Surveillance-Driven Regulation

China's approach to AI regulation is intertwined with national security, economic strategy, and state surveillance. The Personal Information Protection Law (PIPL, 2021) is comparable in scope to GDPR but lacks independent judicial oversight.

The Chinese government actively promotes:

- Facial recognition for public monitoring,
- AI-enhanced censorship,
- Social credit systems.

Recent regulations like the Algorithmic Recommendation Rules (2022) require tech firms to ensure algorithms align with socialist values, avoid promoting addiction, and register them with authorities.

China's model is centralized and control-oriented, prioritizing state goals over individual autonomy or civil liberties.

4. India: Fragmented and Emerging Legal Response

India's legal framework is still nascent and fragmented. Key developments include:

- The Digital Personal Data Protection Act, 2023 (DPDPA) which offers data rights and fiduciary obligations, though with broad exemptions for state actors
- Guidelines by NITI Aayog and MeitY promoting responsible AI ethics, but lacking binding force.
- Courts like in K.S. Puttaswamy v. Union of India (2017) and Shreya Singhal v. Union of India (2015) laid strong foundations for digital rights, but no jurisprudence has yet addressed AI-specific harms.

India is at a critical juncture, where rapid AI deployment risks outpacing legal safeguards, particularly in biometric surveillance, facial recognition, and predictive governance.

 ISSN: 2582-6433

5. Summary Table: Comparative Overview

Aspect	EU	US	China	India
ain AI Law	Act (Proposed, 2021)	federal AI Law	PL, Algorithmic Rules	ne yet; DPDPA 2023 applies
proach	ghts – based, risk – tiered	ctoral, innovation – driven	ate – centric, control - oriented	nerging, fragmented
blic Accountability	gh	edium	w	edium (Judicial activism)
n on Harmful AI	s (Unacceptable risk systems)			explicit bans
tomated Decision Rights	ticle 22 GDPR	mited	mited	t addressed under DPDPA

KEY REGULATORY CHALLENGES IN INDIA

India is at the crossroads of a digital revolution driven by Artificial Intelligence (AI), yet its regulatory architecture is fragmented, reactive, and underdeveloped. While the nation has made strides through data protection reforms and policy papers on AI ethics, critical legal gaps remain. This section identifies the principal regulatory obstacles confronting India in developing a robust AI governance framework.

1. Absence of an AI-Specific Statute

   Despite AI being deployed in sectors such as criminal justice (facial recognition), public welfare (Aadhaar-linked benefits), and employment (algorithmic hiring), India lacks a comprehensive AI-specific law. The Digital Personal Data Protection Act, 2023 (DPDPA) governs data but does not address algorithmic accountability, explainability, or liability in AI-induced harm.

2. Limited Judicial Guidance on AI Issues

   Unlike in the United States where courts have begun adjudicating AI-related due process and bias issues (People v. Loomis), Indian jurisprudence has not yet squarely addressed AI harms. While the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) affirmed data privacy, no case has applied these principles directly to algorithmic decision-making, leading to a legal vacuum.

 ISSN: 2582-6433

3. Weak Oversight Mechanisms

   There is no centralized AI regulatory body in India. Existing agencies like MeitY (Ministry of Electronics and Information Technology) offer only policy-level recommendations. The NITI Aayog's reports on "Responsible AI" are non-binding and lack statutory force.

4. Broad State Exemptions under DPDPA

   Section 17 of the DPDPA allows sweeping exemptions for government surveillance, undermining the very purpose of data protection. This becomes especially dangerous when AI tools are used in policing, predictive governance, or biometric authentication, where there is no independent oversight or grievance redressal mechanism.

5. Inadequate Redressal Mechanisms for Algorithmic Harm

   There are no statutory remedies for individuals harmed by AI systems, whether due to bias, opacity, or incorrect automated decisions. The Consumer Protection Act, 2019, and the IT Act, 2000 offer some recourse but are ill-suited for complex, autonomous, and adaptive AI technologies.

6. Lack of Algorithmic Transparency and Audit Obligations

   Developers and deployers of AI systems in India are not legally obligated to disclose how their algorithms function. This creates opacity in systems that affect rights—from credit scoring to recruitment—and violates fundamental principles of natural justice and procedural fairness.

7. Deficient Public Awareness and Consultation

   AI policy development has largely remained technocratic, with limited public involvement. The lack of formal public consultation mechanisms or citizen engagement in AI law-making leads to low trust and minimal democratic accountability.

8. Fragmentation Across Sectors

   Regulatory oversight is currently divided across sectors (e.g., RBI for finance, TRAI for telecom), with no unifying AI liability or ethical standard. This fragmented approach prevents consistent enforcement and may lead to regulatory arbitrage.

SUGGESTIONS

Based on the empirical findings, public sentiment, comparative legal analysis, and doctrinal research, the following legal, institutional, and policy-level suggestions are proposed to regulate Artificial Intelligence (AI) effectively and ethically in India:

1. Enactment of a Comprehensive AI Legislation

 ISSN: 2582-6433

India should introduce a dedicated AI Act that clearly defines high-risk AI systems, mandates algorithmic transparency, and establishes liability standards for developers, users, and deployers. Drawing from the EU's AI Act model, such legislation must be risk-tiered and rights-centric.

2. Mandate Human Oversight in High-Stakes Domains

   AI systems used in criminal justice, healthcare, surveillance, and public welfare should operate only under human supervision. Human-in-the-loop or human-on-the-loop frameworks must be made legally binding to safeguard fundamental rights and due process.

3. Institutionalize AI Impact Assessments (AIA)

   Before deployment, high-risk AI systems should undergo Algorithmic Impact Assessments to evaluate their bias risks, legal implications, and societal effects. These assessments must be made publicly accessible and reviewed by independent experts.

4. Establish a Central AI Regulatory Authority

   India must establish a statutory Artificial Intelligence Regulatory Commission (AIRC) to oversee licensing, auditing, grievance redressal, and enforcement of AI-related laws. This authority should include legal scholars, technologists, civil society members, and ethicists.

5. Impose Algorithmic Transparency Obligations

   AI developers and platforms must be required to disclose the logic, limitations, and data inputs of high-risk systems. This includes the obligation to maintain auditable logs and provide explanations for automated decisions affecting rights.

6. Public Participation and Stakeholder Consultation

   AI regulation must be a participatory and democratic process, not limited to policymakers and tech companies. Public consultation forums, citizen panels, and civil society hearings must be institutionalized in the legislative process.

7. Enhance Digital Literacy and AI Awareness

   Government bodies, in partnership with academic institutions and media, should launch nationwide digital literacy programs to educate citizens about their rights, risks, and remedies in AI environments—particularly in vernacular languages.

8. Integrate Ethical Design Principles

   India must promote ethics-by-design in AI development through enforceable standards for non-discrimination, inclusiveness, data minimization, and privacy-by-default. Certification schemes for AI ethics compliance should be introduced before market

 ISSN: 2582-6433

release.

9. Foster International Collaboration

   India should engage with global AI alliances, such as OECD's AI Policy Observatory, and harmonize its AI laws with international standards to ensure interoperability, accountability, and innovation within democratic boundaries.

10. Amend Existing Laws to Address AI Harm

    Until a comprehensive AI law is enacted, relevant statutes such as the Consumer Protection Act, IT Act, and DPDPA should be amended to include explicit provisions for algorithmic accountability, bias redressal, and data protection in AI applications.

CONCLUSION

The integration of Artificial Intelligence (AI) into legal, administrative, and socio-economic structures marks a defining shift in how societies operate, make decisions, and safeguard rights. While AI brings undeniable efficiency, predictive power, and scalability, it also introduces unprecedented legal, ethical, and democratic challenges. This research set out to explore these challenges not only through doctrinal analysis but also by engaging public opinion—a vital yet often overlooked dimension in the development of AI policy.

The empirical findings revealed a robust public demand for accountability, transparency, and fairness. A significant majority favored a shared liability model, emphasizing that responsibility for AI-induced harm must be distributed among developers, users, and manufacturers. Respondents consistently rejected opaque and autonomous AI decision-making in sensitive domains such as criminal justice, highlighting the need for human oversight and explainability.

Public opinion also resonated with constitutional values such as equality and privacy. The concern over algorithmic bias reflected a strong social justice orientation, aligning with jurisprudential precedents like Navtej Singh Johar v. Union of India and Puttaswamy v. Union of India. Similarly, the preference for rights such as the right to be forgotten, and support for data sovereignty laws, indicates a growing public awareness of digital rights in the algorithmic age.

At the global level, the comparative study demonstrated that India lags behind regions like the EU in establishing a comprehensive, enforceable AI governance model. While the Digital

 ISSN: 2582-6433

Personal Data Protection Act, 2023 is a step forward, it falls short in addressing the full spectrum of AI-related legal risks—particularly in the domains of algorithmic accountability, discrimination, and due process.

Therefore, the way forward lies in crafting a unified, participatory, and ethically grounded legal framework. Such a framework must be informed by global best practices but rooted in the constitutional culture and social realities of India. This includes new legislation, institutional oversight, public participation, and digital literacy—pillars essential to ensuring that the AI revolution remains democratic, inclusive, and just.

This research concludes that AI regulation in India must be built not only on technical expertise but also on the lived experiences and normative aspirations of its people.

LIMITATIONS OF THE STUDY

Despite the comprehensive scope and empirical methodology adopted, this study acknowledges certain limitations that may influence the generalizability and depth of its findings:

1. Limited Sample Size

   The empirical data is based on a sample of 37 respondents, which may not fully capture the diversity of public opinion across India's varied socio-economic and cultural landscape. Larger and demographically stratified samples would offer more representative insights.
2. Urban-Centric Bias

   Most responses were collected from urban and semi-urban populations with higher digital literacy. The views of rural populations—who are increasingly subjected to state-driven algorithmic systems such as biometric welfare—may remain underrepresented.
3. Self-Reported Data

   The study relies on self-reported survey data, which may involve bias, including social desirability bias or lack of deep technical understanding of AI among respondents.
4. Rapidly Evolving Legal Landscape

   AI technology and its legal governance are evolving rapidly. As of the writing of this paper, new legal developments (such as updates to the EU AI Act or judicial rulings in India) may not be fully captured.

 ISSN: 2582-6433

5. Limited Jurisdictional Comparison

   While the study compares the EU, USA, China, and India, it excludes several other important jurisdictions like Canada, Brazil, and Japan that offer valuable AI regulatory insights.

   These limitations, however, do not undermine the core findings of the research but indicate areas for future empirical expansion and deeper doctrinal engagement.

FINDINGS

This study arrived at the following key findings:

1. Strong public demand exists for an AI-specific regulatory framework in India, with a majority supporting shared accountability and mandatory oversight mechanisms.
2. Public sentiment reflects concerns over algorithmic bias, privacy infringement, and unaccountable surveillance systems, particularly in criminal justice and public governance.
3. There is moderate awareness about existing legal protections like the Digital Personal Data Protection Act, 2023, but low confidence in its adequacy for AI regulation.
4. Comparative analysis reveals that India's approach is still reactive and fragmented, unlike the proactive, rights-based framework proposed by the EU.
6. Public consultations, legal literacy, and transparency mandates are essential elements missing from India's current AI governance discourse.
7. The ethical concerns voiced by respondents—including fairness, inclusivity, and redressability—align with constitutional guarantees under Articles 14, 19, and 21
8. The study shows that law must keep pace with technology and must be grounded not just in expert discourse but in the aspirations and fears of its citizens.

REFERENCES

1. European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final, 2021.
2. Ministry of Electronics and Information Technology (MeitY), Government of India, India AI Strategy: Responsible AI for All, NITI Aayog, 2021. Available at: https://www.niti.gov.in/sites/default/files/2021-07/RAI204July21.pdf

 ISSN: 2582-6433

3. Government of India, The Digital Personal Data Protection Act, No. 22 of 2023. Available at: https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023
4. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1.
5. Navtej Singh Johar & Ors. v. Union of India, (2018) 10 SCC 1.
6. People v. Loomis, 881 N.W.2d 749 (Wis. 2016).
7. Donoghue v. Stevenson, [1932] AC 562 (UKHL).
9. Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap," Columbia Science and Technology Law Review, Vol. 51, 2019.
10. Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015.
11. Federal Trade Commission (FTC), AI and Algorithms Guidance, United States Government, 2020. Available at: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ai-and-algorithms
12. OECD AI Policy Observatory, AI Principles and Policy, 2023. Available at: https://oecd.ai
13. Karen Yeung, "A Study of the Implications of Advanced Artificial Intelligence for Law and Society," Yale Journal of Law & Technology, Vol. 34, 2022.
14. China's Cyberspace Administration, Regulations on the Administration of Algorithm Recommendation Services, March 2022.
15. United Nations Human Rights Council, The Right to Privacy in the Digital Age, A/HRC/39/29, 2018.
16. Shreya Singhal v. Union of India, AIR 2015 SC 1523.