LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH
ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume IV | Special Issue I

2026

Special Issue on the International E-Conference on

"Law in the Age of Artificial Intelligence: A Fundamental Perspective"

Organised by KES' Shri J. H. Patel College of Law, Mumbai, on 24 January 2026

Official Publication Partner: LawFoyer International Journal of Doctrinal Legal Research

DOI: https://doi.org/10.70183/lijdlr.2026.v4si1.16

KES' Shri. Jayantilal H. Patel Law College

About the College

KES' Shri. Jayantilal H. Patel Law College is committed to nurturing and empowering students through quality legal education. The college provides an inclusive and academically enriching environment that encourages students to excel in their studies, participate in co-curricular activities, engage in research, and develop a strong sense of civic responsibility.

The college is affiliated to the University of Mumbai, approved by the Bar Council of India, NAAC accredited with 'B++' grade, and ISO 9001:2015 certified. It offers programmes including B.A. LL.B., LL.B., LL.M., and specialised diploma courses.

With qualified and experienced faculty, a strong academic environment, moot court training, research activities and modern infrastructure, the institution seeks to prepare responsible, skilled and socially conscious legal professionals equipped to meet the challenges of a rapidly changing world.

The college functions under the aegis of Kandivli Education Society (KES), an institution established in 1936 with a long-standing commitment to quality, inclusivity and value-based education.

Affiliation	University of Mumbai
Recognition	Approved by the Bar Council of India
Accreditation	NAAC accredited 'B++'
Certification	ISO 9001:2015 certified

Kandivli Education Society

Established 1936

Kandivli Education Society (KES), established in 1936, has grown from a small educational initiative into a dynamic educational institution serving thousands of students.

With a legacy of quality, inclusivity and value-based learning, KES has expanded its academic presence across various disciplines. Its educational institutions are committed to providing meaningful learning opportunities and fostering academic, professional and personal development among students.

KES' Shri. Jayantilal H. Patel Law College is one of its prominent institutions dedicated to legal education. Through academic excellence, research, practical learning and co-curricular engagement, the college seeks to empower students with the knowledge, skills and values necessary to contribute meaningfully to society.

Educational Commitment

- Quality and inclusive education
- Value-based learning
- Academic and professional development
- Research and practical learning
- Holistic and future-ready education

Law in the Age of Artificial Intelligence

A Fundamental Perspective

About the International Conference

The International Conference on "Law in the Age of Artificial Intelligence: A Fundamental Perspective" provided an academic platform to examine the transformative impact of Artificial Intelligence on law, legal systems, governance and society.

The conference explored emerging legal and ethical questions relating to Artificial Intelligence, including intellectual property, authorship and ownership, liability, data privacy, cybersecurity, criminal justice, evidence law, human rights, ethics and accountability. It addressed the implications of Artificial Intelligence for legal education, commercial law, regulatory frameworks, policy development, research and scholarly communication.

The conference brought together academicians, research scholars, legal professionals and students to present research, exchange ideas and engage in interdisciplinary discussions. It encouraged meaningful academic dialogue and contributed towards the development of effective, ethical and inclusive legal responses to the rapidly evolving Artificial Intelligence landscape.

Conference	International Conference
Theme	Law in the Age of Artificial Intelligence: A Fundamental Perspective
Date	24 January 2026
Time	10:00 AM onwards
Mode	Online
Organised by	IQAC, Student Research Society and Library Committee
Publication Partner	LawFoyer International Journal of Doctrinal Legal Research [ISSN: 2583-7753]

Principal's Message

KES' Shri. Jayantilal H. Patel Law College

It gives me immense pleasure to welcome all academicians, research scholars, legal professionals and students to the International Conference on "Law in the Age of Artificial Intelligence: A Fundamental Perspective."

Artificial Intelligence is transforming the way societies function and is increasingly influencing legal systems, governance, professional practices and education. These developments bring significant opportunities as well as complex legal, ethical and social challenges.

This conference provided a valuable platform for intellectual exchange and interdisciplinary dialogue on emerging issues such as data privacy, intellectual property, liability, criminal justice, human rights, ethics and the governance of Artificial Intelligence. The scholarly contributions and discussions during the conference encouraged deeper understanding and promoted responsible approaches to the use of Artificial Intelligence.

I extend my best wishes to all the speakers, researchers, presenters, participants and members of the organising team for a meaningful and intellectually enriching conference.

Dr. Viral Dave
I/c. Principal
KES' Shri. Jayantilal H. Patel Law College

Organising Committee

International Conference on Law in the Age of Artificial Intelligence

I/c. Principal	Dr. Viral Dave
Convenor	Mr. Mahavir Mandot
Co-Convenors	Dr. Shweta Vijendra Pathak Ms. Priyanka Khakhadia Ms. Deepanshi Chandarana

Organised by IQAC, Student Research Society and Library Committee

KES' Shri. Jayantilal H. Patel Law College, Mumbai

Papers presented at the conference are published in the Special Issue of the LawFoyer International Journal of Doctrinal Legal Research [Volume IV, Special Issue I, 2026]

ENTANGLED THREADS: FORGING DATA PRIVACY, CYBERSECURITY, AND AI GOVERNANCE IN INDIA'S ALGORITHMIC FRONTIER

Viraj Tupe[1]

I. ABSTRACT

Artificial Intelligence (AI) has developed at a very fast rate, and this has significantly changed the way governance, commerce, healthcare, and judicial administration in India take place. Although AI-powered technologies are likely to provide organizations with efficiency, innovation, and economic benefits, they also give rise to sophisticated legal issues related to data privacy, cybersecurity, and regulatory responsibility. This paper presents a critical evaluation of the evolving framework of AI governance in India, particularly examining how data protection and cyber resilience intersect and are governed within an ethical and legal context. It examines the AI Governance Guidelines issued on 5 November 2025 by the Ministry of Electronics and Information Technology (MeitY) under the IndiaAI Mission, and evaluates their effectiveness vis-à-vis binding legal regimes such as the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000. The paper identifies key concerns arising from voluntary compliance models, algorithmic opacity, cross-border data transfers, and emerging cyber threats such as deepfakes and adversarial attacks. Drawing upon constitutional principles under Article 21 and the evolution of judicial thought, including the White Paper on Artificial Intelligence and the Judiciary (2025) prepared by the Centre for Research and Planning (CRP) of the Supreme Court of India, the study examines how AI governance can establish a balance between technological innovation and the protection of fundamental rights. A comparative analysis of the European Union's Artificial Intelligence Act and the federal approach of the United States is used to derive insights relevant to India's plural and socio-economically diverse context. The paper concludes by proposing specific legal reforms aimed at enhancing enforceability, accountability, and inclusivity in artificial

[1]2nd Semester LLB Student at MGM University, Chhatrapati Sambhajinagar (India).Email: virajtupe71@gmail.com

 (ISSN: 2583-7753)

intelligence regulation, thereby contributing to India's vision of innovation-oriented development in pursuit of Viksit Bharat.

II. KEYWORDS

Artificial Intelligence Governance; Data Protection; Cybersecurity; Digital Personal Data Protection Act; Article 21.

III. INTRODUCTION

Artificial Intelligence represents a new age of technological revolution in the twenty-first century, significantly altering legal frameworks, modes of governance, and human interactions worldwide. In India, AI-based technologies are increasingly deployed across sectors such as digital payments, healthcare diagnostics, welfare delivery, surveillance, predictive policing, and judicial administration. The introduction of AI in these areas reflects India's desire to embrace technology as a catalyst for economic growth and streamlined administration. Nonetheless, this widespread adoption has also generated serious concerns regarding data privacy, cybersecurity, and the adequacy of existing legal frameworks.

The Government of India has recognised both the opportunities and risks associated with AI and, in November 2025, published the AI Governance Guidelines as part of the IndiaAI Mission. These Guidelines adopt a principles-based approach focusing on responsible development, human-centricity, accountability, and safety. However, despite being a significant policy initiative, they lack enforceability, which raises concerns regarding their practical applicability and their consistency with binding statutory frameworks such as the Digital Personal Data Protection Act, 2023 (DPDPA) and the Information Technology Act, 2000 (IT Act).

The central legal dilemma, therefore, is whether AI regulation in India can effectively reconcile data privacy protection and cybersecurity requirements with constitutional values. This paper examines whether the current regulatory framework in India is capable of addressing emerging technological risks without stifling innovativeness and inclusive development.

 (ISSN: 2583-7753)

This paper is structured as follows. Following the Introduction, the paper sets out its Research Objectives, Research Questions, and Research Methodology in order to clarify the scope, purpose, and doctrinal-comparative approach of the study. The first substantive section examines the theoretical framework of AI governance and its constitutional foundations. The second section analyses the legal framework governing data privacy and cybersecurity in India, including the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, and the Information Technology Act, 2000. The third section evaluates the India AI Governance Guidelines, including their principles and institutional architecture.

The fourth section explores the relationship between AI and fundamental rights. The fifth section provides a comparative analysis of regulatory approaches in the European Union, the United States, and Japan. The final sections identify emerging challenges, including synthetic content, deepfakes, and AI-related cyber risks, and propose reform-oriented recommendations, followed by a concluding analysis.

A. Research Objectives

The present study aims to examine the adequacy of India's emerging artificial intelligence governance framework in addressing concerns of data privacy, cybersecurity, and constitutional accountability. It seeks to evaluate the relationship between non-binding AI governance principles and binding statutory regimes such as the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000. The paper further aims to assess whether India's current regulatory approach sufficiently protects fundamental rights under Article 21 while permitting responsible technological innovation.

B. Research Questions

1. Whether India's present AI governance framework adequately addresses the intersection of data privacy, cybersecurity, and constitutional rights.
2. Whether voluntary AI governance guidelines can effectively operate alongside binding legal regimes such as the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000.

3. How far Article 21 and the right to privacy provide a constitutional foundation for regulating AI-driven surveillance, profiling, and automated decision-making.
4. What reforms are necessary to strengthen accountability, enforceability, and inclusivity in India's AI governance framework.

C. Research Methodology

This paper adopts a doctrinal and comparative legal research methodology. It relies on primary legal sources including the Constitution of India, the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, relevant rules, governmental guidelines, and judicial decisions, particularly Justice K.S. Puttaswamy (Retd.) v. Union of India. The study also examines policy documents such as the AI Governance Guidelines under the IndiaAI Mission and the White Paper on Artificial Intelligence and the Judiciary. A comparative approach is used to analyse regulatory models adopted in the European Union, the United States, and Japan, with a view to identifying lessons relevant to India's legal and socio-economic context.

IV. THEORETICAL FRAMEWORK OF AI GOVERNANCE

AI governance refers to the legal, ethical, and institutional structures that regulate the creation, deployment, and utilisation of artificial intelligence systems. It encompasses principles such as transparency, accountability, fairness, privacy, and security. Unlike conventional technologies, AI systems are adaptive and autonomous in nature, as they are capable of learning from data and making decisions with minimal human intervention. These characteristics challenge traditional regulatory approaches that are based on predictability, human control, and clear attribution of responsibility.

The normative foundations of AI governance are rooted in data privacy and cybersecurity. AI systems depend on large volumes of both personal and non-personal data, which are often collected and processed across multiple platforms and jurisdictions. Cybersecurity, on the other hand, provides the technical and legal mechanisms required to protect AI systems from risks such as data breaches, manipulation, and cybercrime. Effective governance therefore requires the integration

of these dimensions to ensure that AI systems operate in a lawful, ethical, and secure manner.

In India, the constitutional basis for data protection was firmly established in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, AIR 2017 SC 4161[2], where the Supreme Court unanimously recognised the right to privacy as an intrinsic component of the right to life and personal liberty under Article 21 of the Constitution of India. The judgment further laid down the proportionality test, which requires that any restriction on privacy must satisfy four conditions: legality, the existence of a legitimate aim, necessity, and proportionality in the strict sense.

This proportionality framework is particularly significant in the context of AI governance, especially in relation to AI-driven surveillance, profiling, and automated decision-making systems. The deployment of such technologies by the State must therefore be supported by a clear legal basis, pursue a legitimate objective, and ensure that less intrusive alternatives are considered. Moreover, the extent of data collection and algorithmic intervention must remain proportionate to the intended purpose, thereby preventing excessive intrusion into individual privacy and safeguarding fundamental rights.

V. LAW OF DATA PRIVACY AND CYBERSECURITY IN INDIA

The Indian legal framework governing data privacy and cybersecurity is principally constituted by the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, the Information Technology Act, 2000, and allied rules and regulatory directions. Consent-based processing of personal data, purpose limitation, data minimisation, storage limitation, security safeguards, breach notification, and accountability are among the core principles underlying the DPDPA framework. The DPDP Rules, 2025 operationalise the Act by providing procedural and compliance requirements, including notice obligations, consent-management mechanisms, processing of children's data through verifiable consent, data-principal rights, breach-intimation processes, and the functioning of the Data Protection Board of India.

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

A further difficulty arises in relation to erasure obligations. While data protection law may require deletion of personal data once the specified purpose is fulfilled or where a valid request for erasure is made, trained AI models may retain statistical patterns or inferred representations derived from such data. This creates a technical and legal challenge commonly described as the problem of 'machine unlearning', where removal of a particular data point from the original dataset may not fully eliminate its influence from a trained model. Consequently, compliance with erasure and purpose-limitation obligations in AI systems requires not merely deletion from databases, but also auditable data-governance practices, dataset provenance records, retraining protocols, and technical standards for assessing whether personal data continues to influence model outputs

Therefore, the DPDP Rules, 2025 strengthen India's binding data-protection architecture but also expose the gap between conventional privacy compliance and AI-specific technical realities. Consent, purpose limitation, and erasure are meaningful only when AI developers and deployers maintain traceable datasets, transparent consent records, and mechanisms for responding to data-principal rights even after data has been incorporated into model-development pipelines. In the absence of AI-specific implementation standards, the DPDPA framework may remain difficult to enforce against opaque and continuously evolving AI systems

The DPDPA and the DPDP Rules, 2025 together represent a major development; however, their practical application in the context of AI systems remains complex. AI technologies frequently depend on large-scale datasets, including personal data collected for purposes different from subsequent model training, fine-tuning, profiling, or automated decision-making. This creates tension with purpose limitation and consent requirements, because repurposing datasets for AI training may exceed the purpose for which consent was originally obtained. The requirement of verifiable consent is especially significant where personal data of children or vulnerable users may form part of datasets used by AI developers, platforms, or data fiduciaries

The cybersecurity framework under the Information Technology Act is supplemented by the Information Technology (Amendment) Act, 2008, which introduced Section

43A[3] imposing liability for failure to implement reasonable security practices, as well as the SPDI Rules, 2011,[4] which prescribe standards for handling sensitive personal data. In addition, the CERT-In Directions, 2022[5] issued under Section 70B of the Information Technology Act, 2000 mandate that specified cybersecurity incidents must be reported within six hours.

However, these provisions have not been specifically tailored to AI systems, which are vulnerable to unique threats such as model inversion attacks, data poisoning, and adversarial manipulation. The absence of AI-specific cybersecurity requirements creates regulatory gaps, particularly in high-risk sectors such as fintech, healthcare, and law enforcement.

VI. INDIA AI GOVERNANCE GUIDELINES: AN APPRAISAL

The India AI Governance Guidelines issued in November 2025 under the IndiaAI Mission set out seven foundational principles, known as the 'Seven Sutras': Trust is the Foundation, People First, Innovation over Restraint, Fairness & Equity, Accountability, Understandable by Design, and Safety, Resilience & Sustainability. These principles draw upon the Reserve Bank of India's Framework for Responsible and Ethical Enablement of Artificial Intelligence in the Financial Sector, commonly referred to as the FREE-AI Committee Report, released in August 2025. While this lineage strengthens the Guidelines' grounding in sectoral regulatory experience, it also indicates the need for careful adaptation when applying the sutras beyond finance to other high-risk contexts such as healthcare, law enforcement, and welfare delivery. The principles are broadly aligned with international best practices; however, their voluntary nature limits their effectiveness. Compliance depends largely on self-regulation by developers and deployers of AI systems, with no clear mechanisms for enforcement or penalties, which raises concerns regarding "governance washing" and lack of accountability.

[3] Section 43A of the Information Technology Act, 2000
[4] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[5] CERT-In Directions dated 28 April 2022 issued under Section 70B (6) of the Information Technology Act, 2000

The Guidelines also propose an institutional framework comprising the AI Governance Group (AIGG), the Technology & Policy Expert Committee (TPEC), and the AI Safety Institute (AISI), intended to support coordination, expert advisory input, evaluation, and safety oversight. The TPEC is designed to advise the AIGG on technical and policy matters, including emerging AI capabilities, associated risks, regulatory gaps, and evolving governance priorities. However, their lack of statutory backing, along with the absence of mandatory algorithmic auditing and sector-specific standards, creates gaps in enforceability and may weaken data protection and cybersecurity objectives.

A. The Legal Approach Towards AI and Fundamental Rights

In India, the judiciary has taken a tentative yet evolving role in the development of AI governance. In 2025, the White Paper on Artificial Intelligence and the Judiciary, prepared by the Centre for Research and Planning (CRP) of the Supreme Court of India, highlighted the use of AI tools to improve judicial efficiency in areas such as translation, legal research, and case management. Notable examples include SUPACE (Supreme Court Portal for Assistance in Court Efficiency), SUVAS (Supreme Court Vidhik Anuvaad Software), TERES (AI-based transcription), and LegRAA (Legal Research Analysis Assistant). At the same time, the paper emphasised the need for human oversight to prevent errors, bias, and violations of fundamental rights.

Courts have consistently held that technological advancement cannot operate at the cost of constitutional guarantees. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court established the principles of proportionality and necessity in cases involving infringement of privacy. These principles apply equally to the use of AI systems by the State, particularly in contexts such as surveillance, predictive policing, and welfare delivery.

At the same time, practical concerns have emerged, including instances of AI hallucinations in Indian courts, where reliance on incorrect or non-existent precedents has been observed. Such developments reinforce the need to embed constitutional safeguards within AI governance frameworks, ensuring that automation does not weaken accountability or undermine the dignity and rights of individuals.

B. Comparison of EU and United States

The European Union and the United States provide contrasting models of AI regulation. The European Union's Artificial Intelligence Act adopts a risk-based approach, classifying AI systems into unacceptable risk, high risk, limited risk, and minimal risk categories, with stricter obligations imposed on high-risk systems. This model prioritises accountability and consumer protection, but may create compliance burdens that are difficult to replicate in developing economies In contrast, the United States follows a decentralised and innovation-oriented approach, relying on executive orders, sectoral guidance, and existing regulatory frameworks. This approach shifted further in 2025 when Executive Order 14110 of 30 October 2023, titled *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, was revoked and replaced by Executive Order 14179 of 23 January 2025, titled *Removing Barriers to American Leadership in Artificial Intelligence*. The 2025 order reflects a more deregulatory and pro-innovation orientation by directing federal agencies to identify, revise, or rescind AI-related policies that may hinder American AI leadership. While this model promotes flexibility and competitiveness, it has been criticised for offering comparatively weaker and less uniform safeguards for individual rights

India's approach lies between these models. In addition, Japan's Act on the Promotion of AI-Related Technologies (May 2025) adopts a voluntary, non-binding framework that encourages innovation while promoting responsible practices, making it a closer comparator to India. Given India's socio-economic diversity and federal structure, a hybrid model combining sector-specific regulation for high-risk AI systems with flexible, principles-based governance may be more suitable.

VII. NEW PROBLEMS OF AI GOVERNANCE

India faces several challenges that complicate AI governance. The spread of deepfake technologies threatens electoral integrity, individual dignity, and public confidence. Earlier regulatory responses, including MeitY advisories issued in 2023 under the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, operated largely as cautionary and compliance-oriented directions to intermediaries. However, the regulatory position has since evolved into a more formal and binding framework

through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 10 February 2026 and brought into effect from 20 February 2026.

These amendments specifically address synthetically generated information, including AI-generated or deepfake content, and impose obligations relating to prominent labelling, metadata or provenance-based identification, and expedited takedown of unlawful content within three hours, thereby substantially strengthening India's intermediary-governance response to synthetic media The use of algorithmically biased datasets also risks reinforcing social inequalities, particularly affecting disadvantaged groups. In welfare delivery systems, for instance, Aadhaar-linked biometric authentication failures have resulted in exclusion from food ration benefits, highlighting the real-world impact of algorithmic bias. The digital divide further exacerbates cybersecurity vulnerabilities, exposing rural populations to information misuse and cyber fraud.

Additionally, the cross-border nature of AI supply chains complicates enforcement and liability. AI systems often involve multiple stakeholders across jurisdictions, making it difficult to determine responsibility for harm. The lack of clear legal frameworks for liability attribution in AI-related harms remains a significant concern in the Indian context.

VIII. AI GOVERNANCE AND INCLUSION IN A SOCIO-ECONOMIC CONTEXT

Indian artificial intelligence governance cannot be judged solely on technological and regulatory efficiency, but must also be evaluated through the lens of socio-economic inclusion. The digital ecosystem in India is marked by significant inequality in access to technology, digital literacy, and cybersecurity awareness. While urban centres increasingly benefit from AI-enabled services, rural and marginalised populations continue to face structural barriers in accessing and safely using such technologies. This disparity raises concerns regarding substantive equality and fairness in the deployment of AI systems.

When used in welfare distribution, biometric authentication, and credit assessment, AI systems may disproportionately affect vulnerable populations in cases of failure. Denial of essential services can occur due to automated exclusions, data errors, and biased datasets without adequate grievance redressal mechanisms. In such circumstances, breaches of data privacy and cybersecurity are directly linked to issues of dignity and livelihood, thereby implicating Article 21 of the Constitution.

Although inclusiveness and fairness are recognised as guiding principles under the AI Governance Guidelines, they are not backed by enforceable obligations. In the absence of mandatory impact assessments and transparency measures, AI systems risk reinforcing existing socio-economic inequalities rather than mitigating them. Governance frameworks must therefore incorporate social impact assessments, community-level consultation, and accessibility standards to ensure that AI-driven systems remain equitable and constitutionally compliant.

IX. REFORM-ORIENTED RECOMMENDATIONS

India needs to implement a balanced and enforceable AI governance system that incorporates data privacy, cybersecurity, and constitutional accountability to address the complex challenges posed by artificial intelligence. The following reforms aim to strengthen the existing regulatory architecture while preserving innovation.

To begin with, the Information Technology Act, 2000 needs to be reviewed to include AI-specific cybersecurity requirements, particularly for high-risk AI systems in sensitive sectors such as healthcare, finance, law enforcement, and public services. These amendments should mandate third-party cybersecurity audits, adversarial testing, and risk disclosure requirements to ensure resilience against emerging threats such as data poisoning and model manipulation.

Second, the Digital Personal Data Protection Act, 2023 should be supplemented with detailed provisions governing automated decision-making and profiling. Individuals affected by AI-driven decisions must be provided with meaningful rights to explanation, audit, and redressal. Sector-specific ombudsmen may also be established to reduce the burden on the Data Protection Board of India and improve access to remedies.

Third, institutional mechanisms should be strengthened through the establishment of a National AI Incident Repository under CERT-In. Such a repository would record AI-related data breaches, algorithmic failures, and cybersecurity incidents in a structured and anonymised manner, thereby enabling transparency, policy learning, and evidence-based regulatory responses.

Further, a clear legal framework for liability attribution in AI-caused harms must be developed. Given the involvement of multiple stakeholders such as developers, deployers, and data providers, the law should define responsibility based on the degree of control, foreseeability of harm, and nature of deployment, in order to ensure accountability without discouraging innovation.

Lastly, sustainable AI governance requires capacity-building initiatives. Judicial officers, regulators, and public administrators must be trained in AI ethics, data protection, and algorithmic accountability. Industry practices should be aligned with constitutional and regulatory expectations by encouraging the adoption of privacy-enhancing technologies and secure-by-design AI systems through appropriate policy incentives.

X. CONCLUSION

Artificial Intelligence has created new opportunities and legal challenges in India. Although the AI Governance Guidelines are a step toward a proactive approach to policymaking, voluntary adherence alone is insufficient to safeguard data privacy, cybersecurity, and constitutional values. A balanced framework combining legally binding norms, ethical principles, and innovation-friendly policies is therefore essential.

It is equally important to anchor AI governance within the constitutional framework of Article 21, which guarantees the right to life and personal liberty, including privacy and dignity. The recommendations proposed in this paper particularly those relating to accountability, liability, and regulatory oversight must be understood as mechanisms to give practical effect to these constitutional protections. By aligning AI governance with Article 21 and promoting inclusive development, India can ensure

that technological advancement strengthens human dignity and democratic values rather than undermining them.

XI. REFERENCES

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. The Constitution of India, art. 21.
3. The Digital Personal Data Protection Act, 2023.
4. The Digital Personal Data Protection Rules, 2025.
5. The Information Technology Act, 2000.
6. The Information Technology (Amendment) Act, 2008.
7. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
8. CERT-In, Directions under Section 70B (6) of the Information Technology Act, 2000, 28 April 2022.
9. Ministry of Electronics and Information Technology, Government of India, India AI Governance Guidelines, 2025.
10. Supreme Court of India, Centre for Research and Planning, White Paper on Artificial Intelligence and the Judiciary, 2025.
11. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence.

 (ISSN: 2583-7753)