Artificial Intelligence, Technology, and the Future of Constitutional Rights Reaffirming Fundamental Rights in a Dynamic World

Amandeep Singh
Advocate, District & Sessions Court – Fazilka, and Civil & Taluka Court - Abohar, Punjab - India
doi.org/10.64643/IJIRTV12I6-191353-459

I. INTRODUCTION

The current phase of AI, known as Artificial Narrow Intelligence (ANI), will evolve into future phases like Artificial General Intelligence (AGI) and Artificial Super Intelligence (ASI). Since these AI models will be able to take their own decisions, a major threat lies in who commands them, with what motive, and what they learn from the internet.

The expectation of peace from AI is uncertain, considering that humans, who are often the most violent beings on Earth, destroying the ecosystem for personal benefits. training these systems. For the betterment of mankind, there is an urgent need to draft appropriate and effective laws with a proper framework to protect fundamental rights globally.

AI and associated technologies directly or indirectly impact constitutional rights like liberty, equality, privacy, and dignity. In India, the present situation is critical. In the name of digital and technological advancement, the government is proceeding rapidly by linking identity proofs and services, such as Aadhaar, APAAR, and FASTag.

“This centralization means that personal information - including biometrics (eye scan, fingerprints), date of birth, gender, phone number, address, bank accounts, PAN, driving license, and other registration certificates - is all linked to one source via the internet.”

This situation represents a critical risk, not just mere criticism, as uncontrolled and unaware governance may lead towards upcoming disasters and potentially build the foundation for severe digital crimes, including digital theft, digital extortion, digital kidnapping, digital blackmail, and unauthorized disclosure of privacy.

The Constitution of India, adopted in 1950, was never intended to be a static document. Its inherent strength lies in its dynamic character, enabling continuous reinterpretation by the judiciary to meet the evolving societal and technological realities of the nation.

II. DETAILED DESCRIPTION

AI is a force capable of both unprecedented advancement and unforeseen dangers, creating a fundamental tension in modern society.

1) In case if AI is a Friend

AI’s ability to process vast, complex data quickly, it offers wide range of dramatic improvements across various sectors:

- Revolutionizing Research: AI accelerates scientific, mathematical discoveries by analyzing massive datasets in very short intervals of time, it is also helping in research to find various patterns and it can predict outcomes faster than humans. AI is also capable of drug discoveries and climate modelling.

- Transforming the Legal System: AI tools can instantly search and analyze millions of case laws and statutes in short time. This type of automation speeds up the legal research, and helps to manage judicial timelines. It promotes access to justice

through projects like the Supreme Court's SUVAS [1] translation software.

2) In case if AI is a Foe

The same power that enables efficiency also enables total surveillance and control:

- Black Box Problem: Many AI systems are like "black boxes." When an algorithm makes decisions, it keeps the process secret. As a result, individuals cannot understand why the decision was made, which directly challenges their rights to due process and an explanation.
- Systemic Bias: AI systems learn from data that reflects historical human biases like gender or caste or war etc. When these AI are deployed in public services, the algorithms of these AI systems automatically repeat and amplify discrimination, which is the violation of the fundamental right to equality before the law.

3) Global Approaches to Handle AI

The major global powers are regulating AI, highlighting why this comparison shows that India must act quickly and clearly:

- The European Union has adopted the AI Act, a comprehensive law that categorizes AI systems by their level of risk and imposes tough requirements on companies that build and sell high-risk AI. This approach focuses on strict laws and frameworks to make control over AI service providers as well operators.
- United States' approach relies on principle-based guidelines that focus on general concepts like ensuring non-discrimination and giving users a right to know how a decision was reached. This global difference highlights the necessity for India to adopt proactive state regulation—a clear, forward-looking legal structure.
- Union of India is actively planning and working on ways to control, and regulate AI. Government of India is on a governance system that ensures transparency in the control of AI and technologies. At this stage India is aiming to balance the innovation with safety and ethical use of AI.

This approach largely favours a pro-innovation stance, preferring to avoid immediate, strict legislation. Currently, control is exerted indirectly through comprehensive data protection laws like the Digital Personal Data Protection (DPDP) Act, 2023, which limits the personal data available for AI training purposes. Furthermore, continuous efforts are underway to implement the risk-based controls and advisories to prevent specific harms, such as deepfakes and algorithmic bias, while increasing demand for assurance of algorithmic accountability [2]across critical sectors.

Supreme Court of India is acutely aware of the constitutional fundamental rights implications, using landmark judgments like Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) to establish strong judicial guardrails and ensuring that any state or private use of AI must satisfy the rigorous tests of legality, necessity, and proportionality.

4) Threat of Malafide Governance and Digital Coercion

- Surveillance and Tracking: Uncontrolled governance can take command of AI in their own hands at any time, because AI and its sister technologies can easily be used as an instrument for mass control and for surveillance. The combination of tools like Facial Recognition Technology (FRT) [3] with centralized, linked identity databases (Aadhaar, APAR, FASTag, and

---

[1] **SUVAS** - Supreme Court Vidhik Anuvaad Software

[2] Algorithmic Accountability is the legal and technical obligation to provide auditable evidence demonstrating how an AI system arrived at a decision

[3] **FRT** is a biometric surveillance tool that raises unique constitutional concerns regarding anonymity and freedom of movement (Article 19). Studies show FRT often exhibits higher error rates when applied to minorities, thus exacerbating systemic discrimination (Article 14).

GPS) enables the state to conduct real-time, comprehensive tracking of citizens of the nation. This mass surveillance is clear violation of Constitutional fundamental rights.

- Command-Based Control and Discrimination: Beyond tracking, AI systems can be commanded to show specific, biased results or control access to essential public services. This power can be abused to exclude or discriminate against certain groups, for example, by unfairly denying welfare or employment opportunities. Such actions directly impact constitutional rights like equality and liberty by using technology to reinforce systemic bias.
- Individual Misuse and Compromising Justice: The concentration of data and AI's power to create convincing lies (deepfakes) opens the door to devastating digital crimes. Criminals can use AI to scrape sensitive, linked personal data and then create highly realistic deepfakes of an individual engaged in wrongful acts. The threat of disclosing this fabricated content becomes a potent tool for blackmail and coercion. This threat extends directly to the justice system, as AI-driven blackmail could be used to influence judges, advocates, and key legal personnel, compromising their independence or forcing the alteration of legal documents and evidence. This represents a direct assault on the integrity and independence of the judiciary, a cornerstone of the Constitution.

5) The Constitutional Imperative in India

- Protecting Privacy: The Right to Privacy is fundamental under Article 21 of the Indian Constitution, and its protection relies on the rigorous application of the three-pronged test established by the Supreme Court: Legality, Necessity, and Proportionality. Any AI-driven state intrusion must meet these three standards.
- Ensuring Equality and Fighting Algorithmic Bias: The use of biased algorithms violates the guarantee of Equality before the Law. To prevent the institutionalization of discrimination, India must mandate Algorithmic Accountability and give citizens the right to contest any adverse decision made by an AI.
- Freedom of Expression and Private Power: Dominant private social media platforms use opaque AI to censor content, curbing the Freedom of Expression. This requires the application of constitutional duties to private actors, forcing them to adhere to principles of transparency and fairness in their automated censorship.

6) Towards Digital Dignity: A Regulatory Blueprint for India

India's current data protection laws, while a crucial first step, are insufficient for addressing the specific, systemic risks posed by advanced AI. The Digital Personal Data Protection (DPDP) Act, 2023, primarily focuses on data handling; it does not contain the necessary mechanisms to tackle AI's unique harms, such as algorithmic opacity, embedded bias, and the potential for mass state misuse. Therefore, India urgently needs a proactive, rights-based state regulation to bridge this governance gap.

❖ The Path to Protection

To establish effective control, India must move beyond general principles and establish a dedicated, structured legal and institutional framework designed specifically for AI.

- Adopting a Risk-Based Approach: India should adopt a risk-based approach similar to the European Union's pioneering AI Act. This strategy acknowledges that not all AI poses the same threat; thus, regulatory burdens should correspond to the potential harm.
  - Classification by Risk: AI applications must be legally classified in three classes - unacceptable risk, high risk, limited risk.
  - Mandatory Assessments: High-risk AI applications defined as those used in critical sectors like judicial systems, health services, law enforcement, and welfare distribution— must undergo mandatory Fundamental

Rights Impact Assessments (FRIAs) [4] before deployment.

These assessments are vital to proactively identify, mitigate, and publicize the risks of bias, privacy invasion, and discrimination before the systems can cause societal harm.

- Establishing an AI Commission of India: Effective regulation requires sustained, expert oversight that lies outside the political influence of the ministries deploying the AI. Therefore, an independent regulatory body needs to be established on a proper, strong, and strict framework.
    - This proposed body, the "AI Commission of India," should be established with statutory independence and equipped with multidisciplinary expertise like legal, technical, and ethical.
    - The mandate must include the authority to enforce accountability, conduct ex-ante and ex-post audits of algorithms, impose strict financial penalties for non-compliance, and issue binding technical standards. This institutional muscle is necessary to ensure AI is governed by the rule of law.

❖ Assuring "Digital Dignity" through Legal Mandates:

The ultimate purpose of this regulatory blueprint is not simply to manage risk, but to assure "digital dignity[5]." This concept represents the modern extension of the Right to Life under Article 21 into the digital realm, guaranteeing that every citizen retains autonomy over their digital identity and personal narratives.

- Sovereignty and Transparency: For digital dignity to be real, citizens must remain in control of their digital identity and data. This requires a fundamental shift in the power dynamic between the state/platforms and the individual.
    - Mandatory Disclosure of Logic: The frameworks must legally mandate and be able to ensure full disclosure of AI logic for all high-risk systems. The opacity of "black box" systems must be cracked open, ensuring that citizens are not subjected to decisions made by an unknown, unaudited mechanism.
    - Human Oversight and Review: To prevent fundamental rights from being automated away, the regulation must embed human review at all critical decision-making points. This provides an effective appellate mechanism and ensures that technology serves as a tool for human governance, not a replacement for human judgment.

This comprehensive approach affirms that technology must serve human rights, not the reverse, thereby securing the constitutional promise of dignity for every Indian citizen.

III. THE CALL TO ACTION

The judiciary, the legislature, and the citizenry must recognize that this technological frontier demands a "digital constitutionalism." Failure to establish strong, proactive legal boundaries now risks institutionalizing unchecked digital power, potentially leading to a surveillance state where privacy is merely a memory and equality is automated away by biased code. The time for hesitant, reactive policy is over; the future of India's democratic and constitutional promise hinges on the urgent and ethical governance of Artificial Intelligence.

IV. CONCLUSION

[4] FRIA is a pre-emptive policy tool requiring developers and deployers to systematically identify, assess, and mitigate the potential negative effects an AI system may have on constitutional rights (like equality, privacy, and non-discrimination) *before* it is launched into public use.

[5] Digital Dignity is the concept that extends the Right to Life and Personal Liberty (Article 21) into the digital realm, ensuring that technology and automated processes do not diminish an individual's fundamental autonomy, self-determination, or reputation in the interconnected digital society.

The age of Artificial Intelligence presents the ultimate test for the dynamic character of the Indian Constitution. The threats posed by mass surveillance, algorithmic bias, and digital extortion are present realities that exploit the centralized data structure of projects like Aadhaar and Facial Recognition Technology. By legally mandating Algorithmic Accountability and rigorously enforcing the three-pronged proportionality test on all state-led technological projects, India can firmly bridge the gap between technological advancement and constitutional values. The proactive adoption of a comprehensive, rights-based regulatory framework is not just a policy choice but a constitutional necessity to reaffirm fundamental rights and secure the "digital dignity" of every citizen in this dynamic world.

REFERENCES

Books

[1] Barfield, W. The *Future of Human Rights in the Age of Artificial Intelligence*. (Edward Elgar Publishing, (2020)).

[2] Sharda, A. *Digital Dignity: Reimagining Constitutional Rights in the Internet Era.* Oxford University Press, (2021).

National and International Instruments

[3] *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.* The White House, Washington D.C. (2023).

[4] *Regulation (EU) 2024/1689* of the European Parliament and of the Council of 13 June 2024 on harmonising rules on Artificial Intelligence (Artificial Intelligence Act).

[5] *The Constitution of India,* 1950 (as amended).

[6] *The Digital Personal Data Protection Act,* 2023.

Article/Report

[7] Sury, D. *Algorithmic Bias and the Constitutional Challenge to Equality in India.* (Indian Law Review, 6(1), 45-68, (2022)).

[8] Solon, O. *The Secret Biometric Force: How India's Aadhaar Programme Affects Privacy and Security.* (The Guardian, (2018)).

Case Laws

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