

Citation: Dr. Bimaldeep Singh & Ms. Prerna, "Artificial Intelligence and Forensics Investigation in India: A Critical Analysis" St. Soldier Journal of Law and Social Science, Vol. 2:2, July 2026 pp. 7-29

Artificial Intelligence and Forensics Investigation in India: A Critical Analysis

Dr. Bimaldeep Singh

Associate Professor, Dept of Laws, Guru Nanak Dev
University, Amritsar, Punjab.

Ms. Prerna

Research Scholar, Dept of Laws, Guru Nanak Dev University,
Regional Campus, Jalandhar.

I. The rapid development of Artificial Intelligence (AI) technologies has radically altered the way of governance, criminal investigation, judicial administration and forensic science extent in India. Algorithms are interfering with decision-making processes, whether through automated facial recognition systems for confirming the identity, predictive policing, algorithmic content moderation, or AI-enabled cyber-forensic systems. Although this kind of technological integration improves investigation efficiency, scalability, and administrative accuracy, numerous deep evidentiary issues associated with privacy, algorithmic reliability, transparency, and forensic accountability are also brought up. However, its rights-based design, and especially the protection of Articles 14, 19, and 21¹, is able to offer a normative framework that is able to adapt to new digital forensic realities. Identification of informational privacy as a fundamental right and development

¹ *Constitution of India, 1950.*

of the doctrine of proportionality has increased the interpretative powers of the judiciary to deal with harms, data contamination caused by investigative technology².

However, the AI-driven digital forensics have distinct regulatory. Legal and evidentiary issues that are not limited to the traditional data security or data protection issues. In contrast to the conventional administration decisions, AI forensic systems are run by opaque computational structures, probabilistic evaluations, and automated profiling, and may lack any meaningful human supervision. India has in the past few years embraced legal provisions like the *Information Technology Act, 2000*³, and *Digital Personal Data Protection Act, 2023*⁴, in addition to policy-based efforts of enhancing responsible AI development. Nonetheless, these tools do not necessarily treat AI accountability at a holistic level; they mostly focus on the issue of data governance and intermediary liability. The lack of clear legislation on AI specifically brings about regulatory disparity and casts vital concerns about the admissibility of electronic evidence presented by state and non-state actors utilizing high-impact AI systems.

The point of convergence between the application of AI forensic and the rights guaranteed by the Constitution requires a redefinition of the regulatory philosophy. The problem extends beyond the regulation of technology in a digital criminal justice system where algorithmic systems have the ability to determine freedom, reputation, access to opportunities, and democratic discussion. In response, it is vital to study AI from a digital forensic and its evidentiary value perspective to make sure that the technological progress does not contradict the postulates of the rule-of-law, procedural

² Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy” 04:05 *Harvard Law Review* 195 (2007).

³ *Information Technology Act 2000 (Act No. 21 of 2000)*.

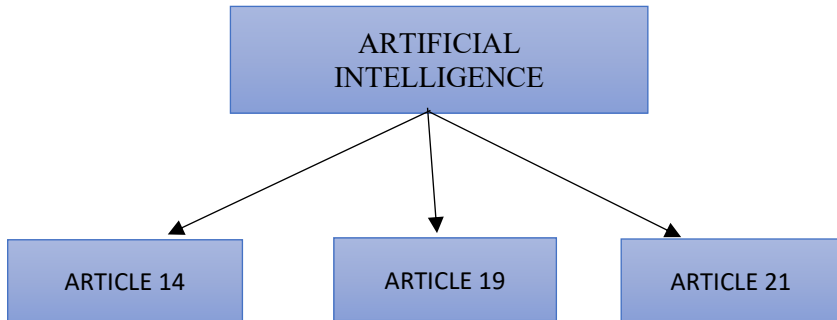
⁴ *Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)*

fairness, and substantive justice. The present study analyses the impact of AI-driven forensic technologies on evidentiary basis, including privacy, equality, freedom of speech and expression, and informational autonomy. It critically evaluates the adequacy of the existing legal framework (especially the cyber regulations) in addressing challenges arising from the deployment of AI forensic systems in criminal justice mechanism. Further a comparative analysis of AI regulatory approaches adopted by the European Union and the United States is undertaken to identify and assess their relevance for a balanced and rights-oriented framework for AI governance in India.

Research Methodology- The study employs a doctrinal and analytical research methodology, relying predominantly on secondary sources such as constitutional provisions, landmark Supreme Court judgments, government policy documents, law commission reports, and scholarly articles. Further, a comparative approach has been employed to analyse international regulatory developments, including the European Union's risk-based AI regulatory model and the United States' sector-specific approach to AI governance. The comparative analysis facilitates the identification of best practices and regulatory principles that may be adapted to the Indian constitutional context. The study is analytical in nature and seeks to critically evaluate existing legal and policy frameworks, identify regulatory gaps, and suggest reforms for developing a constitutionally compliant and rights-oriented framework for Artificial Intelligence governance in India.

II. The regulation of Artificial Intelligence and forensic techniques in India should be based on the constitutional system instead of discussing this issue as a sectoral or technical compliance matter. The normative core of the constitutional

examination of AI-driven forensic systems used by the State or by other actors acting as a private player in the exercise of a public role is made up of articles 14, 19 and 21.



Article 14 - Equality and Algorithms Bias

Article 14 ensures that there is equality before the law and equality of the protection of the laws. Article 14 acquires a new significance in the AI forensic context as a result of the so-called algorithmic bias and automated discrimination in criminal profiling. Trained AI investigative systems might give biased data in biometric identification, face recognition techniques for identification purpose, predictive policing and criminal history matching because of incomplete record. This discrimination need not be overt but it can be indirect in the form of disparate impact. When the biased algorithms are used by state investigative authorities, the constitutional ban on arbitrariness and unequal treatment is applied directly. Besides, non-arbitrariness doctrine, now entrenched in Article 14 jurisprudence, states that state action should be rationale, clear, and a nexus of intelligible differentia towards the objective that is being pursued. Non-transparent algorithmic decision-making in forensic, especially in cases where people lack the benefits or fall under negative repercussions without any scientific explanation of the decision-making principle, is a practice that

threatens to contravene this constitutional requirement. Therefore, constitutional review of AI under Article 14 should go beyond visible classification in order to consider structural bias and lack of scientific explainability and procedural safeguard in forensic based techniques⁵. *Maneka Gandhi v. Union of India* - The Supreme Court expanded the scope of Article 14 by holding that arbitrariness is antithetical to equality. Consequently, AI-driven forensic decisions that operate through opaque 'black-box' algorithms and produce discriminatory outcomes may be vulnerable to constitutional scrutiny on the ground of arbitrariness⁶.

Article 19 – Freedom of Speech and Digital Platforms

Article 19(1)(a) safeguards the freedom of speech and expression but limited to some reasonable restrictions as in Article 19(2)⁷. The AI has a profound impact on online speech ecology in terms of automated forensic tracking, surveillance, deepfakes or tampered electronic evidence. In case such systems are implemented in accordance with state investigative orders or regulatory laws and regulations, constitutional review is inevitable. Even under the governance of the private platform, we should ask whether the dominant digital intermediaries perform some quasi-public functions, which should be obligated by the Constitution. The use of algorithmic moderation can contribute to over-censorship, chilling, or suppressions of speech which is based on discrimination. On

⁵ Ayushi Shreya, "AI, Bias, and The Constitution: A Jurisprudential analysis of Algorithmic Inequality under Article 14" 5:10 *Indian Journal of Legal Review* 873 (2025).

⁶ (1978) 1 SCC 248.

⁷ *Constitution of India, 1950, art 19(2)*.

the other hand, the lack of moderation can contribute to false information and malicious growth⁸.

Shreya Singhal v. Union of India the Supreme Court emphasised that restrictions on online speech must satisfy constitutional standards of reasonableness. The judgment assumes significance in the context of AI-driven surveillance systems, which may suppress lawful speech through automated filtering mechanisms without adequate procedural safeguards⁹.

Anuradha Bhasin v. Union of India - The Court here recognised the internet as an important medium for exercising freedom of speech and expression. Consequently, algorithmic control over online visibility and content dissemination raises important constitutional concerns¹⁰.

Article 21- Right of privacy and informational autonomy

Article 21 warrants safeguarding of life and personal liberty and this has been broadly understood as the right to privacy and informational autonomy. Privacy is the right to be free from covert observation and to select when, how, and to whom one's information is disclose.¹¹ Facial recognition, potentially automated profiling, biometric authentication, and predictive analytics have become a major concern with regard to surveillance, consent, and autonomy. Constitutional recognition of privacy leads to a three-fold obligation of any state action that interferes with personal data; it must be lawful, with a legitimate purpose, and proportionate. In addition to

⁸ Jennifer Cobbe, "Algorithmic Censorship by Social Platforms: Power and Resistance" 34:01, *Springer* 740 (2020).

⁹ (2015) 5 SCC 1.

¹⁰ (2020) 3 SCC 637.

¹¹ S. Sandesh Saravanan and M. Kannappan, "An Overview of the Changing Data Privacy Landscape in India with Regard to the Role of Data Controllers", 119:17 *International Journal of Pure and Applied Mathematics* 920 (2018).

protecting data, procedural fairness and dignity is also included in Article 21. The right to be treated with dignity and informational self-determination require an AI system of high impact to be transparent, open to contestation, and under human oversight¹². *K.S. Puttaswamy v. Union of India* - In the Aadhaar judgment, the Supreme Court reiterated that collection and processing of personal data must satisfy standards of proportionality and necessity. This principle becomes particularly relevant where AI-driven systems rely on large-scale biometric and behavioural datasets¹³.

While Articles 14, 19, and 21 provide a strong constitutional foundation for the protection of individual rights in digital age, their application to Artificial Intelligence-enabled forensic investigation system remains largely interpretative rather than explicitly codified. The existing constitutional framework was developed in an era when algorithmic governance, machine learning, automated decision-making, facial recognition technique and large-scale data analytics were not envisaged. Consequently, courts are often required to extend traditional constitutional doctrines to emerging technological contexts. Although judicial innovations such as the recognition of informational privacy and the proportionality doctrine have strengthened constitutional safeguards, significant uncertainties remain regarding the accountability of scientific evidence, algorithmic transparency, and remedies against automated decision-making. Furthermore, constitutional protections are generally enforced through judicial intervention, which may not always provide timely or effective remedies against rapidly evolving AI-driven harms. Therefore, while constitutional jurisprudence offers a valuable normative framework, reliance solely on constitutional interpretation is insufficient. There is a

¹² Luciano Floridi, *The ethics of Artificial Intelligence*, 27 (Oxford University Press, UK, 1st edn., 2023).

¹³ *AIR (2019) 1 SCC 1*.

pressing need for statutory mechanisms with clear procedural standards regarding the collection, analysis, preservation and admissibility AI- driven digital evidences.

Proportionality and Due Process Doctrine

Proportionality doctrine has become an important tool in constitutional adjudication. Any limitation made to the fundamental rights must serve a valid purpose, use reasonable means, take the least restrictive alternative and maintain a balance between violation of rights and the common good. Proportionality is an auditing mechanism in constitutional law as applied in the realm of artificial intelligence¹⁴. Indicatively, the introduction of the facial-recognition system in the security of social areas must prove the necessity and the least harm¹⁵. Indiscriminate surveillance measures, as implemented by blankets, would not be able to meet this high standard.

The due-process requirements have necessitated the use of reason when arriving at decisions and the right to appeal against unfavorable results. Accountability may not be covered by algorithmic opacities. In the case of AI systems having a significant impact on rights, procedural protections, such as an announcement, clarification, and review, have to be incorporated into the constitutional system. When interpreted together with proportionality and procedural fairness, articles 14, 19, and 21 have the overall effect of requiring AI systems (especially those implemented in the governance sector) to work in a transparent, accountable, and rights-respectful environment.

¹⁴ *What would it take? The potential and limits of proportionality analysis in law available at: <https://www.tandfonline.com/doi/full/10.1080/20403313.2024.2419755> (last visited on April 10, 2026).*

¹⁵ Pete Fussey and Daragh Murray, “Face Recognition Surveillance” 236 (Oxford University Press, UK, 2025).

Although the doctrines of proportionality and due process provide important constitutional safeguards against arbitrary state action, their effectiveness in regulating Artificial Intelligence remains subject to significant practical limitations. The proportionality test presupposes the availability of sufficient information regarding the purpose, functioning, and impact of a regulatory measure. However, AI systems often operate through complex and opaque algorithms, making it difficult for courts, regulators, and affected individuals to assess whether a particular system satisfies the requirements of necessity, proportionality, and least restrictive means. The absence of transparency and explainability may therefore undermine the meaningful application of constitutional scrutiny.

Similarly, due process protections are challenged by automated decision-making mechanisms that frequently function without adequate notice, reasons, or opportunities for review. Individuals affected by algorithmic decisions may be unaware that an AI system has influenced the outcome, thereby limiting their ability to challenge adverse actions. Furthermore, existing constitutional remedies are largely reactive and dependent upon litigation, which may be inadequate in addressing large-scale and rapidly evolving AI-related harms. Consequently, while proportionality and due process remain valuable constitutional tools, their effective implementation in the context of Artificial Intelligence requires complementary statutory safeguards such as algorithmic transparency, mandatory impact assessments, human oversight, and accessible grievance-redress mechanisms¹⁶.

Role of AI in Digital Forensics

¹⁶ Dheeraj Kumar and Navdeep Kaur , “Balancing AI Innovation and Civil Liberties: An Indian Constitutional Perspective” 3:2, *Indian Journal of Law and Society* 62 (2025).

Artificial Intelligence (AI) has significantly transformed digital forensic investigations by enabling the rapid collection, processing, and analysis of large volumes of digital data. Traditional forensic methods often struggle to handle the growing complexity of electronic evidence, whereas AI-powered tools can efficiently identify relevant information, detect patterns, and support investigative decision-making. AI is widely used in cybercrime investigations, malware detection, facial recognition, image and video analysis, and the examination of electronic records. For instance, AI-assisted facial recognition systems may help identify suspects from CCTV footage, while machine learning algorithms can analyse emails, chat logs, and financial transactions to detect fraudulent activities. Similarly, AI-powered forensic tools are increasingly used to detect deepfakes and manipulated digital content, thereby assisting investigators in verifying the authenticity of electronic evidence.

Despite its advantages, the use of AI in digital forensics raises concerns regarding accuracy, transparency, privacy, and accountability. Cases involving AI-based facial recognition errors and the growing misuse of deepfake technology highlight the potential risks associated with excessive reliance on automated systems. Therefore, the integration of AI into forensic investigations must be accompanied by appropriate legal safeguards to ensure the reliability and fairness of forensic outcomes.

III. India currently lacks an individual and extensive Artificial Intelligence in forensic investigations. Rather, AI assisted forensic practices is controlled indirectly by a mix of constitutional principles, cyber laws, data protection laws, criminal procedure laws, the information-technology law and judicial precedents This disjointed structure provokes relevant issues relating to coherence, enforceability, accountability and

admissibility of AI- generated forensic evidence under the criminal justice system mechanism.

Information Technology Act, 2000

Information Technology Act 2000 (IT Act) is the parliamentary act that forms the basis of the legislation on the electronic communication, cybersecurity, and intermediary liability in India. Even though the Act does not directly impact AI implementation, some of its provisions have an indirect impact on AI implementation. Section 43A¹⁷ renders liability of not ensuring the safety of sensitive personal data, thus creating a negligence-based accountability framework. Section 66¹⁸, makes criminal acts related to the computer like unauthorized access and manipulation of data. Also, intermediary liability clauses, especially those dealing with safe-harbour safeguards have a major contribution in controlling digital platforms deploying AI-based content moderation and recommendation systems.

A significant limitation of the Information Technology Act, 2000 is that it adopts a technology-neutral approach, which, while beneficial for flexibility, fails to adequately address the unique risks posed by Artificial Intelligence. The Act was designed primarily to facilitate electronic commerce and address cyber offences, rather than regulate autonomous and predictive technologies capable of influencing individual rights and public decision-making. As a result, the legal framework focuses on post-harm liability rather than preventive regulation. In the context of AI, constitutional harms such as discriminatory profiling, automated exclusion from welfare benefits, or predictive surveillance may occur even in the absence of a conventional cyber offence. The Act therefore

¹⁷ *Information Technology Act 2000* (Act No. 21 of 2000) s. 43a.

¹⁸ *Information Technology Act 2000* (Act No. 21 of 2000) s. 66.

lacks the normative and institutional mechanisms necessary to address the constitutional implications of algorithmic governance. This reveals a structural gap between traditional cyber law regulation and the emerging realities of AI-driven decision-making.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021¹⁹ also provide the due diligence requirements, grievance-redressal policies and procedure of content takedown. But they do not bind themselves with the transparency requirements with regard to automated systems or require algorithmic audits. These Rules raise important constitutional concerns regarding freedom of speech and expression under Article 19(1)(a)²⁰. The increasing reliance of digital platforms on AI-driven content moderation systems may result in over-removal of content, erroneous takedowns, and suppression of lawful speech. Since automated moderation tools often prioritise efficiency over contextual understanding, they may fail to distinguish between harmful content and legitimate political, academic, or journalistic expression. Furthermore, the broad compliance obligations imposed on intermediaries may incentivise platforms to adopt excessive censorship in order to avoid regulatory consequences. This creates a risk of private enforcement of speech restrictions without adequate procedural safeguards or judicial oversight. Consequently, while the Rules aim to promote a safer digital environment, their implementation through automated systems necessitates a careful balance between platform accountability and the constitutional guarantee of free expression.

Digital Personal Data Protection Act, 2023

¹⁹ *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.*

²⁰ Constitution of India, art. 19(1)(a).

The main law of the data-governance in India is the Digital Personal Data Protection Act, 2023 (DPDP Act)²¹. It governs the treatment of digital personal data and puts in place responsibilities of data fiduciaries, such as lawful treatment, limitation of purpose, minimisation of data, accuracy, and limitation of storage, and security measures. The rights that data principals are granted include access to information, correction, and erasure of data, grievance-redressal and the right to withdraw consent. Nevertheless, the DPDP Act is oriented on data control and not on the accountability of algorithms. It does not explicitly provide an impact assessment of automated decision-making and codifies a right to explanation in a situation where AI systems have a substantial impact on people. Although data protection is an obligatory aspect of AI regulation, it is not enough to solve the problem of, although not limited to, algorithmic bias, nonexistence, or automated profiling of non-personal data.

Justice K.S. Puttaswamy v. Union of India - Although the DPDP Act advances data governance, it does not fully operationalise the privacy guarantees recognised in Puttaswamy, particularly in relation to automated decision-making, algorithmic profiling, and explainability requirements²².

***Bharatiya Sakshya Adhiniyam, 2023*²³**

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) represents a significant step towards recognising the growing importance of electronic evidence in the administration of criminal justice. The Act accords legal recognition to electronic and digital records, thereby strengthening the evidentiary framework for

²¹ *Digital Personal Data Protection Act 2023* (Act No. 22 of 2023).

²² (2019) 1 SCC 1.

²³ The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).

digital forensic investigations. In an era where Artificial Intelligence (AI) is increasingly used for analysing electronic data, identifying patterns, authenticating digital content, and assisting forensic examinations, the provisions of the BSA assume particular significance. AI-assisted forensic tools may facilitate the examination of emails, digital documents, CCTV footage, social media communications, and other forms of electronic evidence. However, the growing use of AI also raises concerns regarding the authenticity, reliability, and admissibility of AI-generated forensic outputs. While the BSA provides a legal foundation for the acceptance of electronic evidence, it does not specifically address issues relating to algorithmic decision-making, explainability, or the evidentiary value of AI-generated findings. Consequently, the increasing integration of AI into digital forensic investigations necessitates the development of clear legal standards to ensure the accuracy, transparency, and fairness of electronically derived evidence.

Government Policies on AI (Initiatives on AI by NITI Aayog and IndiaAI)

The AI governance in India has been more of a policy-led approach as opposed to statute-driven approach. The strategy documents of the government focus on responsible AI, ethical implementation, and growth driven by innovation. The principles that are promoted by policy frameworks include transparency, fairness, accountability, and inclusivity. The policy instruments are however not binding as far as they are not converted into statutory requirements or rule regulations. In addition, regulators of specific sectors (banking, telecommunications, health, etc.) can also provide advisory norms regarding digital systems, however, there is no consistent cross-sector AI control authority at the moment. In a nutshell, the current legal system of India covers elements of

AI governance, including data protection, cybersecurity, and the intermediary liability but is not currently a comprehensive constitutional system of AI regulation.

IV. Artificial Intelligence has structural, normative, and institutional issues that go beyond the usual regulatory issues. However, in contrast to the conventional technological tools, AI systems have decision-making independence, predictive features, and adaptive learning algorithms which may have a considerable impact on personal rights and democracy. Within the context of the Indian constitution, these issues cannot be considered just as technological dangers but they may also be viewed as possible violations of basic rights.

Algorithmic Discrimination and Bias

The AIs are trained by historical data that can support the currently existing social inequalities. The biased datasets can recreate or even increase structural discrimination in a country such as India where disparities exist based on caste, gender, and economic as well as regional lines. AI-based recruitment technologies can be used to disproportionately discriminate against those with a marginalised background where past recruitment data is based on ostracizing practices. Likewise, predictive policing or credit-scoring systems can be discriminatory against certain groups of people. These consequences raise grave constitutional issues in Article 14 especially when used by the state authorities. Difficulty is in identifying and establishing algorithmic bias, particularly in cases of proprietary or opaque decision-making logic. The discriminatory effects can be hidden without the process of regular audits and the necessity to disclose, which compromises the equality assurances.

Data Surveillance and Privacy Risk

Artificial intelligence (AI) technologies rely on the massive aggregation of data, profiling, and behavioural analytics. The threat posed by mass surveillance technologies, such as facial-recognition devices, biometric authentication applications, and real-time tracking solutions, is a significant threat to the informational privacy and autonomy. The combination of AI and surveillance systems of the state increases the likelihood of omnipresent monitoring without proper protection. Unselective gathering of information, lack of the purpose restriction and long-term data storage can provoke the unwarranted intrusion into the individual freedom. Moreover, in the private-sector AI applied by commercial products, mass-scale profiling of behaviour is conducted on a regular basis to help serve targeted advertising, financial rating, predictive analytics. The totality of this is the generation of digital dossiers that can affect decisions, opportunities, and reputational status²⁴. The constitutional issue is to make sure that surveillance practices meet the legality, necessity, and proportionality requirements and do not allow the abuse or overreach.

Lack of Transparency and Accountability

Opacity is one of the greatest risks that relate to AI systems. Most AI models are considered black boxes, i.e. they generate a response without the ability to explain the reasoning behind it to the people who were affected²⁵. The non-explanability of automated systems reject loan applications, limit access to online services, decide who qualifies as welfare recipients, or designate people as security threats, which harms the procedural fairness. In the absence of transparency systems,

²⁴ Mr. Sanjit Sarkar, "A Study Of Artificial Intelligence (Ai) In Commerce: Opportunities, Challenges And Future In India" 13:01, *International Journal of Creative Research Thoughts* 182 (2025).

²⁵ Bram Vaassen, "AI, Opacity, and Personal Autonomy" 35:88, *Springer Nature Link* 88 (2022).

people are left without substantial opportunities to oppose unfriendly decisions. In addition, the regulators are not necessarily technologically able or legally empowered to audit algorithmic systems. Lack of accountability is also compounded by the situation in which the developers, deployers, data providers, and platform operators are decentralized in the responsibilities. It makes it difficult to ascertain liability in torts of harm hence undermining its enforcement.

Gaps in the Indian Law Regulations

The existing Indian laws on data protection and intermediary liability are relevant to the present situation but do not cover high-risk AI systems in their entirety. Algorithms impact is not statutorily required to assess the impact or be independent audited, or classified as a risk. Sectoral regulators are siloed and the control over it is not centralised in any single authority that is strictly in charge of AI regulation. This disintegration causes confusion among the innovators and lack of protection among the citizens. Moreover, the solutions that can be offered to the victims of automated decision-making are still limited and procedurally cumbersome. The constitutional writ litigation may not be practically available in every situation especially when considering the actions of private actors. The main issue, in short, is the lack of alignment between fast-changing AI technologies and a regulatory framework that is reactive and data-driven, as opposed to a rights-driven regulatory framework. The deployment of AI will lead to the normalisation of lack of transparency, discrimination and surveillance in the democratic governance without structural reform based on the principles of the constitution.

V. A comparative analysis of the models of regulation in the world provides important understanding of the way

constitutional democracies are adapting to the Artificial Intelligence. Although the regulations philosophies vary in jurisdictions, some of the common patterns are the categorization of risks, transparency requirements, accountability requirements, and the need to have human oversight.

European Union European Union Risk-Based Regulatory Model

The European Union²⁶ has embraced a holistic and systematic regulation of AI by a risk-based regulation framework. The AI systems under this model fall into these categories, which include unacceptable risk, high risk, limited risk, and minimal risk. Those systems that present unacceptable risks are banned, and those that present high risks are exposed to restrictive compliance obligations. Risky AI systems are required to meet requirements such as risk management frameworks, data governance guidelines, technical documentation, human oversight, transparency, and conformity testing before new systems are put into the market. Also, the European data protection regime requires impact assessments of data protection and acknowledges protection against purely automated decision-making with a severe impact on individuals.

United States Sectoral and Executive Approach

By contrast, the United States has a more sector-specific and decentralised regulatory system. Instead of trying to pass one general AI law, the regulation is spread over the federal government, sectoral regulators, and executive orders. Recent

²⁶ REGULATION (EU) 2024/1689 of The European Parliament and The Council available at:

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (last visited on May 09, 2026).

executive orders focus on responsible AI development, national security protection, and voluntary promises of the private technology companies²⁷. The federal agencies have been promoted to perform impact assessment, improve the procurement standards, and deal with algorithmic discrimination in their areas of jurisdiction. Nevertheless, the lack of a single statutory framework brings inconsistency in the enforcement process and the disparity in protecting rights among sectors.

Applicability of Comparative Models to India

In the case of India, both models cannot be transplanted wholesome. The European model provides a risk-classification system and a compulsory compliance framework which is consistent with the constitutional values of proportionality and accountability. Nonetheless, its administrative intricacy might be something that needs contextual adjustment. The United States model focuses on the need to have sectoral flexibility and support innovation, but might not be ideal in overcoming structural rights vulnerabilities in an emerging democracy with severe social inequalities. A regulatory approach to AI in India needs to be a synthesis of both models, namely: implementing a risk-based classification system of high-impact AI applications, introducing compulsory transparency and impact analysis conditions, and having high standards of institutional regulation based on constitutional principles.

VI. In the light of the transformative and disruptive nature of AI systems, regulation can not be limited to data protection

²⁷ *Executive Order 14110 of October 30, 2023- Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* available at : <https://www.govinfo.gov/content/pkg/DCPD-202300949/pdf/DCPD-202300949.pdf> (last visited on May 19, 2026).

compliance or intermediary liability standards. An even rights based and constitutionally matching structure is a necessity.

The right to equal opportunity in regulation

India regulation of artificial intelligence should be clearly traced on Article 14, 19, and 21 of the Constitution. The rights-based approach will force high-impact AI systems, especially those being used in governance, public services, finance, employment, and surveillance to undergo constitutional review, utilizing the criteria of legality, necessity, proportionality, and procedural fairness. A framework of this nature would include compulsory Algorithmic Impact Assessment (AIAs) on high-risk systems, frequent bias audits, transparency reports, and requirement of strict documentation²⁸. Victims of automated decision-making should have a right to explanation, review and correction which should be enforceable.

Institutional Machinery and Checks and Balances

The governance of AI needs to be institutionally strong. India can think of having specialised regulatory body, or a coordinated oversight system which would work together with the current regulators like Data Protection Board and sectoral authorities. The oversight bodies ought to be given authority of audit, inspection, investigation and imposing penalties. The procurement of AI systems by the government should be subject to the accountability and transparency requirements, such as third party audit and publication of risk evaluations. In addition, there should be coordination of regulation to avoid jurisdiction fragmentation. Having a centralised structure, which introduces a standard set of rules, but at the same time,

²⁸ *Understanding the Algorithmic Impact Assessments Requirements in Legal Frameworks* available at: <https://treatya.com/algorithmic-impact-assessments-requirements/> (last visited on May 21, 2026).

permits adoptions based on the sector, will optimise coherence and legal certainty.

Recommendations

To realize these constitutional controls over AI, the following are the suggested reforms:

1. A comprehensive legal framework regulating the use of Artificial Intelligence in digital forensic investigations and evidence analysis is required.
2. AI-based forensic tools and techniques should get periodic audits for their validation certificate and for enhancing scientific credibility.
3. There should be a set of guidelines regarding the collection, preservations, analysys and admissibility of AI- generated evidences to maintain the chain of custody in criminal investigation.
4. The AI- forensic techniques should be governed and regulated by strict safeguards to prevent the misuse, bias and violations of privacy.
5. The use of AI in surveillance and predictive policing should be made specifically dependent on the fulfillment of the requirements of legality, necessity, and proportionality.
6. Transparency and explainability requirements should be imposed on AI systems used by law enforcement agencies so that decisions and outcomes generated by such systems can be independently scrutinised and challenged.
7. Robust mechanism should be established to protect individual privacy and personal data during AI-surveillance, facial recognition techniques, biometric techniques.
8. There needs to be heightened redressal of grievances to help in offering remedies i.e the right to challenge the accuracy of such AI- produced evidences.

9. Specialised training should be provided to judges, prosecutors, investigating officers, and forensic experts regarding the operation, limitations, and evidentiary implications of AI technologies.
10. A multi-regulatory body comprising of legal experts, forensic experts, technologists, engineers and data protection specialists should be established to oversee the deployment of AI in digital forensic investigations

These reforms will harmonize the level of technology to the democratic accountability and the rule of law.

Conclusion

The growth of artificial intelligence in the areas of governance, investigations and evidence mechanism is a momentous change in the interaction of technology with constitutional rights. Although the constitutional jurisprudence of India is robust in terms of offering a normative basis such as under Articles 14, 19 and 21, the existing statutory framework is still disjointed and inadequate to overcome AI-specific hazards. Algorithms bias, the growth of surveillance, lack of transparency, and fragmentation of regulation are all reasons that stress the need to change. Practical experience shows that active, risk-based regulation in connection with imposing enforceable transparency requirements is plausible and justified.

An AI regulatory framework founded on the principles of constitution needs to go beyond the reactive litigation and introduce proactive safeguards, institutional regulation, and protect rights of the victims. India can promote the idea of technological governance that is constitutional by instilling constitutional values in the approach to innovation, thus preventing the cost of equality, liberty, dignity, and democratic integrity. The future path of AI-based regulation in India will remain to be decided on the possibility of lawmakers, courts,

and regulators to balance the blistering technological advancement and sustainable constitutional obligations. The most sustainable way of going forward is a rights-oriented method that is calibrated.