REGULATING ARTIFICIAL INTELLIGENCE – A COMPARATIVE LEGAL FRAMEWORK FOR AI GOVERNANCE

Dr. Adv. Vandana A. Bhosale Assistant Professor, School of Legal Studies (Law), Sanjay Ghodawat University, Atigre, Kolhapur-416118, Maharashtra. Email: vandana4005@gmail.com Mob: 9420244000

Dr. Adv. Sampada Pise Incharge Principal, Shripatrao Chougule Vidhi Mahavidyalaya, Malvani Kotoli, Email: principalscvmmk@gmail.com Mob: 9420449920

---

1. INTRODUCTION

1. Background on Artificial Intelligence (AI)

Artificial Intelligence (AI) is a stream in computer science whose aim is to make machines intelligent, so that they can accomplish tasks that generally need human intelligence. Such tasks are speech comprehension, image acknowledgement, finding solutions, strategic planning, and learning from experience. AI enables robots and computers to behave more humanly and assist us in multiple disciplines. The purpose of AI is to simplify life and make it more convenient through development of systems that are capable to think, learn, and improve by them.

Yet, the speedy development of AI technologies has also generated a number of legal, ethical, and social issues. Data privacy, algorithmic bias, transparency deficiency, job replacement, and potential abuse of autonomous systems are some of the problems that indicate an immediate need for a well-defined regulatory system. AI systems, particularly those dealing with key decision-making processes, can affect essential rights and social structures, necessitating regulation as a priority.

2. Importance of AI Regulation

Regulating AI is crucial to facilitate that its development and application are reliable with the values of neutrality, accountability, clarity, and human rights. Otherwise, AI systems can perpetuate current inequalities, be a threat to personal freedom, and be used with ill intent (e.g., deepfakes, autonomous weapons).The necessity of AI regulation can be highlighted in the following points:

- Protecting fundamental rights namely privacy, equality, and freedom of expression.
- Ensuring accountability for decisions made by AI-driven systems.
- Promoting ethical AI development that serves public interest and democratic values.
- Encouraging innovation while managing associated risks.
- Establishing trust among stakeholders including consumers, developers, and regulators.

3. Purpose and Objectives of the Study

The main aim of this study is for examining changing scenario concerning AI regulation and contrast legal methods embraced by various jurisdictions, with a specific focus on India. The goals are:

- To evaluate current and pending legal structures that regulates AI in India and other important jurisdictions like European Union (EU), United States (US), China, Japan, Canada, and India.
- To determine the strengths, weaknesses, and shortfalls of existing regulatory models.
- To identify how India can craft a well-balanced regulatory strategy that encourages innovation while protecting rights and ethical principles.

- To offer policy recommendations on the basis of comparative knowledge to inform an effective and inclusive AI governance framework for India.

4. Research Methodology: Comparative Legal Analysis

The research paper follows a comparative legal approach which entails analysis and comparison of the legal system of various nations to establish best practices, regulatory gaps, and evolving global norms. This entails:

- Analyzing statutory laws, policy documents, judicial rulings, and ethical guidelines.
- Comparing the risk-based regulatory model EU, US, China, Japan, and Canada along with, market-based approach of these countries, and the evolving regulatory efforts in India.
- Assessing how cultural, economic, and political considerations drive legal reactions to AI in every jurisdiction.

Such an approach enables understanding of what lessons India could derive from cross-country experiences as well as mitigate its own peculiar socio-economic realities.

1.5 Scope and Limitations

Scope:

- The research concentrates on AI governance from a legal perspective, looking into laws, policies, and ethics.
- It incorporates a cross-comparison of the EU, US, China, Japan along with India.
- A focus is laid on central legal concerns such as data privacy, liability, discrimination, and usage in law enforcement.

Limitations:

- The research does not cover the technical operations of AI algorithms widely, as the primary focus remains on legal and policy aspects.
- Given the rapidly developing nature of AI, it is possible that new regulatory developments may arise after the completion and publication of this paper.
- The analysis is limited to publicly available legal documents and policy records. It does not include internal government deliberations or classified projects, which may also have a bearing on the governance landscape.

2. KNOWLEDGE OF AI AND ITS LEGAL CHALLENGES

2.1 Definition and Scope of AI

AI relates to computer systems having capacity to execute tasks that would otherwise need human intelligence. Some of the activities cover learning, reasoning, problem-solving, perception, and language knowledge. The AI system may be rule-based or self-learning through algorithms like machine learning and deep learning. AI has its scope across various sectors such as healthcare, financial management, education, agriculture, crime prevention, including defense.

2.2 Types of AI

- **Narrow AI (Weak AI):** Programmed for a single task, e.g., voice assistants (Siri, Alexa), recommendation engines, or face recognition. Narrow AI is the most widely utilized type of AI today.
- **General AI (Strong AI):** Theoretical systems with capacity to comprehend, learn, and utilize knowledge on a broad variety of tasks—on par with human intelligence.

- **Super AI:** A hypothetical notion of AI that is superior to human intelligence in every category—reasoning, creativity, and emotional intelligence. It is speculative and much talked about in philosophical and moral arguments.

2.3 Most Important Legal and Ethical Issues

a. Liability and Accountability

Perhaps the most significant legal question around AI is about holding someone guilty when an AI platform is destructive—whether the maker, the builder, the operator, or the AI itself? Classical tort law tends to come up short when faced with an autonomous system that behaves erratically. Ideas such as "product liability" and "vicarious liability" are being reconsidered everywhere in order to fill this void.

b. Data Privacy and Protection

AI generally depends on large collections of data, such as personal and sensitive data. This poses issues of data privacy, user consent, and data security laws compliance. In India, the Digital Personal Data Protection Act, 2023, provides a framework for lawful handling of data, data fiduciary obligations, and rights of users, which will have a major impact on how AI systems are created and put into effect in the country.

c. AI Bias and Fairness

AI platform can strengthen current social prejudices based on erroneous datasets or biased algorithms. This leads to discriminatory decisions in employment, credit scoring, and law enforcement. AI fairness involves both legal regulation and algorithmic transparency to prevent unequal treatment along gender, caste, race, and socio-economic lines.

d. Intellectual Property and Ownership

AI raises new questions in intellectual property law, for example: Can AI work is copyrighted? Who is the owner of invention or content produced by AI—developers, users, or nobody? Legal jurisdictions disagree on how to treat AI authorship, and legal clarity continues to develop.

e. AI in Justice Administration and Surveillance

The application of AI in anticipating policing, facial recognition, and behavioral analysis causes threats to main rights like freedom of expression, privacy, and due process. In India, particularly, application of facial recognition systems in public areas has been a cause of concern regarding mass surveillance and absence of legal protection.

3. INTERNATIONAL LEGAL REGIMES FOR AI GOVERNANCE

1. AI Regulation in the EU

EU has put forth Artificial Intelligence Act (2021), the globe's very first extensive regulatory framework on AI. It applies risk-based supervisory strategy to categorize AI systems in four types — unacceptable risk, high risk, limited risk, and minimal risk. AI systems of high risk (for example, biometric monitoring, recruitment software, credit scoring) are mandatory to meet stringent regulatory requirements, including human oversight, transparency, and data governance. The General Data Protection Regulation (GDPR) is essential to directives of AI. It contains programmed executive action and assessment provisions in Article 22, which entitles individuals to right not to be subjected to decisions taken exclusively on automatic operations. This converges directly with AI systems applied to employment, banking, and public facilities. The European Commission's High-Level Expert Group on AI produced Ethics Guidelines for Trustworthy AI in

2019 these set out core principles like human agency, privacy, transparency, and non-discrimination.

2. ***Regulation of AI in the US***

US have a sectoral regime of AI regulation with no single federal act that controls AI. Federal bodies e.g. Federal Trade Commission (FTC) track use of AI in consumer markets, targeting deceptive and unfair trade practices, while others such as the FDA oversee AI-powered medical devices. The National AI Initiative Act of 2020 enables coordination and funding for R&D in AI. In addition, proposals like the Algorithmic Accountability Act want to mandate testing and risk management of automated decision systems by corporations. In October 2022, the White House Office of Science and Technology Policy (OSTP) circulated Blueprint regarding AI Bill of Rights, providing non-enforceable rules about equitable and safe AI execution. Yet decentralized structure will often lead to regulatory gaps as well as differences, particularly where privacy and responsibility are involved.

3.3 Governance of AI in China

China's AI governance structure is an expression of modern China's top-down, state-centered governance model, with a focus on national security, industrial dominance, and social control. The government strongly integrates AI policy into overall economic and political objectives. China's National AI Development Plan (2017) aims to make the country a world leader in AI by 2030. This plan pushes AI growth in areas like defense smart cities, healthcare, and education. The Provisions on Administration of Algorithmic Recommendation Services (2022) stands out as a key legal tool. These rules require internet platforms to show their recommendation algorithms. They also ban algorithmic bias and limit misleading content personalization.

China is also a world leader in utilizing AI for mass surveillance, particularly through face recognition technology built into both public security initiatives such as the Skynet and Sharp Eyes programs these networks are sometimes coupled with the Social Credit System, supporting predictive policing and scoring behaviour. Though useful for governance effectiveness, these constitute extremely serious concerns over privacy, due process, and human rights. Critics highlight the lack of independent supervision and low civil society engagement, locating China's AI governance as functional but morally impenetrable.

3.4 Japan: Human-Centric, Balanced Approach

Japan's AI strategy is highly reflective of its social harmony, respect for human dignity, and devotion to technological progress. It is among the earliest nations to explicitly promote a people-centered approach to AI governance. The Ministry of Internal Affairs and Communications' AI Governance Guidelines (2019) emphasize transparency, safety, privacy protection, and empowering users. These are non-binding guidelines followed broadly by industry with voluntary compliance supported by enforcement mechanisms.

Japan's Society 5.0 vision, championed by the Cabinet Office, projects a super-smart society in which digitalization and AI collaborate towards improved quality of life, addressing demographic issues, and enhancing sustainability. It seeks to combine cyberspace with the physical world in order to foster inclusivity and happiness. Japan proactively participates in influencing international norms through the OECD AI Principles, G7 Hiroshima AI Process, and UNESCO Recommendations. It eschews overregulation, given that innovation can flourish best when accompanied by ethical consciousness and public trust.

3.5 Canada: Rights-Based and Transparent Approach

Canada stands out with its rights-based, transparent, and participatory AI governance, prioritizing human rights, democratic accountability, and public sector ethics. Canada was one of the first State to develop a countrywide AI strategy—the Pan-Canadian Artificial Intelligence Strategy (2017)—aiming at research, capacity-building, and responsible innovation. In 2021, Canada launched the Artificial Intelligence and Data Act (AIDA) as peice of Bill C-27, a wide-ranging electronic rights agreement overhaul. AIDA adds regulatory mandatory rules for high-impact AI systems, such as risk mitigation, bias evaluation, impact audits, and transparency disclosures.

One of Canada's distinctive elements is its strict focus on AI transparency in the public sector. The Directive on Automated Decision-Making (2019) necessitates federal body to administered algorithmic impact assessments (AIA) prior to using AI systems in government decision-making.Canada is one of the GPAI co-founders—a multilateral effort toward ethical AI research and international collaboration. Although progressive in its approach, Canada is confronted with issues like delays in the implementation of AIDA, issues regarding enforcement instruments, and jurisdictional conflicts between provinces and the federal government.

4. AI GOVERNANCE IN INDIA: EMERGING LANDSCAPE

India has started its journey of AI governance, embedded in policy initiatives, sectoral experimentation, and infrastructure expansion. However, the nation still does not have a specialized and complete legal framework dealing with AI technologies.

4.1 Role of NITI Aayog's National AI Strategy – #AIforAll

India's roadmap for AI initiated officially with the NITI Aayog 2018 discussion report named National Strategy for AI that envisions a "vision for #AIforAll." National Strategy for Artificial Intelligence sees five sectors which can bring inclusive growth through AI as healthcare, agriculture, education, smart mobility, and smart cities. The strategy urges responsible development, skill development, and ethical application of AI but doesn't have enforceable regulatory standards.

4.2 Digital Personal Data Protection Act, 2023 (DPDPA)

India's DPDPA, 2023 forms foundational regulatory regime for data processing that has direct bearing on AI systems dependent on large-scale personal data.It defines data fiduciary obligations, consent of users, grievance redressal, and substantial penalties for non-compliance. Though not AI-specific, it establishes baseline privacy norms necessary for responsible AI deployment.

4.3 Sector-Specific Use of AI

AI has experienced fast-paced adoption across sectors in India:

Healthcare: AI technologies help in diagnostics (e.g., TB and cancer), telemedicine, and predictive analytics in public health surveillance.

Agriculture: Crop monitoring, pest identification, and climate prediction are done using machine learning through portals such as eNAM and Krishi Vigyan Kendra.

Fintech: AI facilitates fraud monitoring, credit scoring, and automation of customer facilities in digital lending and payments.

4.4 Surveillance and Facial Recognition Use: AFRS and CCTNS

India is putting AI-based surveillance tools into action such as: AFRS (Automated Facial Recognition System): The National Crime Records Bureau (NCRB) has adopted this system. It looks at facial details from live feeds and images to spot identities in databases. CCTNS (Crime and Criminal Tracking Network and Systems): This networked database helps with predictive policing and criminal profiling. These systems raise worries about privacy, consent, and misuse. This is true because there's no clear legal protection or court oversight.

4.5 Indian AI Governance Challenges

a. No Overarching AI Law

India lacks a unified AI law that enunciates rights, duties, or technical guidelines. There is regulatory oversight in bits and pieces and mainly policy-based.

b. Inadequate Enforcement and Accountability Mechanisms

Even where there are regulations such as the DPDPA, enforcement infrastructure is still underdeveloped, and data protection authorities are still being set up.

c. Data Localization and Digital Divide Concerns

The trend towards data localization, while in pursuit of security and sovereignty, can raise compliance costs and impact global AI innovation collaborations. Further, limited internet penetration and digital literacy in rural communities exacerbate the AI accessibility gap, undermining the inclusiveness of "#AIforAll."

5. COMPARATIVE ANALYSIS: INDIA VS INTERNATIONAL FRAMEWORKS

Governance of AI has become one of the principal policy priorities of jurisdictions, yet the regulatory style and maturity of regulations differ extensively among nations. India pushes for AI in its state plan, but still lacks a clear legal structure. On the other hand, places like the EU have put tough wide-ranging rules in place such as the AI Act (2021). Meanwhile, countries like the US, China, and Japan have focused more on specific sectors or ethical guidelines. The following section contrasts India's model of AI governance with these international players on multiple axes.

1. Legal and Regulatory Framework

India's existing legal response to Artificial Intelligence is piecemeal and policy-based. Although significant progress has been made through DPDPA, 2023, and NITI Aayog's National Strategy on AI (#AIforAll), India still does not have a complete and obligatory legislative framework committed to AI regulation. Current legal tools like the Information Technology Act, 2000, only indirectly cover AI-related issues like cyber security and data use, but not necessarily algorithmic accountability or high-risk AI systems. This has resulted in uncertainty in areas like liability, ethical regulation, and transparency.

Conversely, the EU has turn into a world leader through introduction of Artificial Intelligence Act (2021) — a historic legislative tool that follows a risk-management plan to AI system regulation. It categorizes AI applications in terms of danger level and requires high-risk systems to have transparency, human oversight, and conformity evaluations. Complemented by the GDPR, which protects data rights and privacy in AI, the EU system offers a rights-based and precautionary model of AI regulation.

The US has been more decentralized and sector-focused, with federal bodies such as the FDA, FTC, and National Institute of Standards and Technology (NIST) offering direction in their own areas. AI Bill of Rights (2022), while non-binding, sets out ethical standards e.g. data privacy, explain ability, and protection against algorithmic unfairness. Yet, lack of a extensive federal law

renders the U.S. model innovation-led but dispersed, with uneven enforcement across industries and states.

China has embraced a state-led regulatory model, prioritizing national security, social stability, and algorithmic control. Internet Information Service Algorithm Recommendation Regulations (2022) and Cybersecurity Law and Personal Information Protection Law (PIPL) establish a tight regime for the regulation of algorithmic systems, particularly those applied in public debate, fintech, and surveillance. In contrast to the Western paradigms emphasizing individual rights, China's legal framework enforces state dominance over AI systems through algorithm audits, openness requirements, and state regulation.

Japan chose the soft-law route, depending on ethical standards instead of binding laws. Government's Social Principles of Human-Centric AI advocate transparency, fairness, and privacy while permitting space for innovation. This self-regulatory framework inspires industries to use AI responsibly while respecting society's values and avoiding excessive regulation.

Canada has recently moved forward with its governance structure through the draft AIDA, which is element of Digital Charter Implementation Act, 2022. AIDA seeks to control significant effect AI systems by placing obligations on risk assessment, monitoring, and record-keeping. It also requires transparency obligations and bans certain harmful activities like irresponsible use of personal data. Canada's approach falls between the EU's legal strength and US's culture of innovation, balancing rights protection with adaptive regulation.

In short, although India's AI policy demonstrates a desire to use AI for public good, its legal framework is underdeveloped. The EU has adopted a structured and enforceable regulatory model, the US has sectoral oversight, China is pursuing authoritarian-style regulation, Japan focuses on ethical compliance, and Canada suggests a balanced rights-risk approach. To make India's AI deployment safe and inclusive, it has to move from policy to effective legislation, borrowing international best practices and reconciling with local constitutional, technological, and socio-economic contexts.

2. Governance Vision and Regulatory Philosophy

The governance vision and philosophy for AI are vastly different across nations, consistent with their socio-political orders, legal frameworks, and strategic interests. The vision for governance in India rests on economic growth, digital inclusion, and social change. The NITI Aayog's #AIforAll policy framework conceptualizes AI as a solution to overcome core developmental issues in areas namely agriculture, healthcare, and academics. Still, current vision is delivered through sectoral policies and non-binding guidelines. The regulatory philosophy is overwhelmingly innovation-friendly and permissive with an emphasis on investment attraction and developing national AI capability but not much attention given to ethical or rights-based enforcement. The lack of a singular AI law also means that accountability frameworks and ethical principles are advisory and not compulsory.

EU, in comparison, advocates a human-centered and rights-based governance paradigm. EU’s regulatory philosophy prioritizes protection of fundamental rights, democracy, and rule of law, integrating these into its legislative efforts like AI Act and GDPR. EU’s perspective is precautionary and proactive, built on the belief that regulation should precede mass deployment of AI systems to prevent potential harm. The vision for governance focuses on responsible AI, transparency, and ethical governance, making the EU a global leader in setting standards.

In the US, the regulatory approach is market-led innovation and AI research and development leadership. Governance is dispersed, with individual states and federal agencies formulating policies appropriate to their domains. The AI Bill of Rights (2022), although advisory, demonstrates an increasing recognition of the necessity for ethical use of AI, but the general philosophy remains one of minimal government intervention, giving the tech sector a high degree of autonomy. This market-first strategy promotes innovation but may result in lacunae in ethical responsibility and civil rights protections.

China's governance paradigm is closely tied to its state-oriented political framework, in which AI is a strategic national asset. The philosophy of the government in regulation prioritizes control, monitoring, and ideological conformity to direct AI to social governance, economic growth, and national security. Regulations like the Algorithm Regulation Law and PIPL are dual-purpose regulations with both regulatory and political purposes. As opposed to democratic frameworks, China's vision integrates AI into the general social credit system, causing profound global concerns regarding privacy, autonomy, and government overreach.

Japan has a soft-law, morally oriented style of AI regulation. Its vision lies in its "Society 5.0" vision that seeks to achieve a human-oriented, AI-linked society. Human-Centric AI Social Principles furnish moral direction for developers and users, calling for fairness, inclusion, and security. The Japanese government has greater faith in industry self-regulation and public-private partnership than formal legal requirements and prefers gradual rule-making consistent with cultural attitudes and technological optimism.

Canada, on the other hand, presents a blended vision of individual protection of rights and innovation promotion. Canada aims to promote responsible AI development, especially in high-impact systems, by introducing the AIDA. Its regulatory approach centers on risk reduction, algorithmic transparency, and fairness, while fostering collaboration with civil society and indigenous peoples. Canada's approach coincides with international ethical standards but also considers the necessity of legal enforcement and government oversight.

Overall, while nations namely EU and Canada prioritize ethical responsibility and human rights, India and the US prioritize innovation-led models, with India still in the process of transforming into a holistic regulatory approach. China's top-down approach focuses on state control and social management, while Japan's ethical direction model promotes self-regulation and moral duty. In order for India to come up with a strong governance vision, it has to balance development ambitions with ethical protections, drawing lessons from rights-based and innovation-led regulatory approaches all over the world.

3. Risk Assessment and Accountability Mechanisms

Risk assessment and accountability are the basic pillars in making AI systems work ethically, transparently, and harmlessly. Nations around the globe have followed different models based on their legal systems, technological advancement, and policy focuses. India does not have a formal system of categorizing AI risks or making robust accountability structures in place as of now. Though efforts like NITI Aayog's #AIforAll strategy ensure ethical development of AI, they are non-binding. The DPDPA of 2023 offers protection against data processing but does not directly touch on algorithmic transparency or risk assessments for AI systems. Mandatory algorithmic audits or impact assessments for high-risk applications, like facial recognition or AI for

policing, do not exist either. This shortcoming exposes India to untransparent and unaccountable AI applications in sensitive sectors.

Conversely, the EU has adopted risk-based regulatory framework in its seminal Artificial Intelligence Act (2021). The norms categorize AI systems into four part—unacceptable, high, defined, and minimal risk. High-risk systems, likely those applicable in indispensible infrastructure, employment, and biometric monitoring, are required to undergo obligatory conformity assessments, documentation, and regular checks. The EU's regulatory framework provides legal accountability through mandatory human oversight, transparency requirements, and post-deployment reporting.

The US follows a decentralized and sector-specific strategy. Rather than a comprehensive federal AI law, the US relies on structure such as NIST AI Risk Management Framework (2023) and oversight by agencies like Federal Trade Commission (FTC). These guidelines encourage organizations to assess risks related to bias, misuse, and data security but are largely voluntary. Accountability is imposed primarily by consumer protection legislation and litigation, which might not be effective or timely in fast-changing AI environments.

China's regulatory strategy emphasizes state control and social stability. Under the Algorithm Regulation Law of 2022, firms need to perform algorithmic self-testing and report use of recommendation technology to state organs. Platforms must also ensure algorithms don't impair social order and create unwanted content. Real-time monitoring, censorship measures, and stringent penalties assure accountability, according to the priorities of the government to synchronize AI research with national security and ideological needs.

Japan advocates for an ethical and self-regulatory model. Rather than coercive legal measures, Japan has adopted the Social Principles of Human-Centric AI, which urge impartiality, safety, and visibility in AI systems. Corporate are persuaded to voluntarily review the risk of their AI deployments and undertake measures to mitigate such risks. The lack of binding accountability frameworks or enforcement mechanisms weakens this model in terms of discouraging the misuse of AI in high-risk domains.

Canada offers a balanced approach that blends innovation with legal responsibility. The proposed AIDA requires organizations deploying “high-impact systems” to conduct risk assessments, maintain records, and assures that AI model do not cause harm or discrimination. Act also empowers regulators to conduct investigations and impose penalties for non-compliance, reflecting a commitment to transparency, safety, and human rights protection.

In short, although the EU and Canada have made risk governance structured and enforceable through institutions, the US and Japan depend more on sector-specific or voluntary arrangements. China's top-down model places state control ahead of openness, and India remains in the formative stage with no established accountability framework for AI. For India to provide responsible AI deployment, it needs to establish a strong risk classification framework, introduce algorithmic audits, and establish statutory duties that unambiguously allocate responsibility and provide redressal upon harm.

4. ***Transparency and Public Participation***

Transparency and citizen engagement are critical in establishing trust and democratic accountability for AI governance. Such values assist in forestalling the abuse of AI technologies, pushing towards responsible development, and enabling citizens to comprehend and shape how AI impacts their lives. India has achieved some such opening up of discussions around AI via public

consultations, for example, by NITI Aayog, and the National Strategy for AI draft. But these efforts are largely advisory in nature and lack legally enforceable transparency requirements. The newly implemented DPDPA, 2023 makes sure individuals are notified when data is collected, but fails to cover making decisions by AI systems (such as profiling or automated service denials) clearer. Furthermore, there is presently no legal requirement for algorithmic transparency or disclosure by developers as to how AI systems operate, especially in government or policing contexts such as AFRS (Automated Facial Recognition System).

Transparency is a foundation of the AI Act in the EU, which requires explainability, disclosure, and user knowledge for specific AI systems, particularly high-risk systems. Those using AI-based services have to be notified when they are being serviced by an automated system. Public participation is formalized through consultations with stakeholders and public comments on bills under legislative development. In addition, the EU focuses on human review, making AI-driven decisions susceptible to review or challenge.

The United States encourages transparency by sectoral regulation and agency guidance like the FTC, which supports transparent revelation of how AI systems impact consumers. The Blueprint for an AI Bill of Rights (2022) demands algorithmic transparency and public engagement, although it is a non-binding document. Furthermore, public engagement in AI policymaking is increasing through civil society advocacy and congressional hearings, although full laws enforcing transparency are yet to be implemented.

China is more state-centric in its approach to transparency. Although the Provisions on Algorithmic Recommendation Services (2022) obligate platforms to inform users of algorithmic decision-making, the main emphasis is on regulatory access and not on public participation. Citizens lack adequate recourse to comprehend or dispute government-employed AI systems, particularly surveillance ones. Transparency is therefore often restricted to what the state allows.
Japan promotes voluntary transparency through its ethical standards, such as the AI Utilization Guidelines. These guidelines suggest that developers make system limitations and risks public, particularly in applications impacting safety or rights. Although public participation is not required by law, Japan promotes transparency by encouraging industry-initiated consultations and multi-stakeholder discussions in policy development.

Canada, through the drafted AIDA, makes organizations accountable to be open regarding how high-impact AI systems function. The Act further implies public reporting and provides regulatory bodies with authority to require explanation and documentation of AI activity. Furthermore, Canada's AI policy has been informed by public consultations so that greater numbers of civil society and academia can be represented.

In short, the EU and Canada have led the way in institutionalizing transparency mandates as well as public participation mechanisms. The US encourages these values but does not have federal enforcement, whereas Japan and India use soft-law instruments or voluntary disclosure. China, although mandating some disclosures, restricts citizen monitoring in favor of state monitoring. For India to advance, it must establish legally enforceable requirements of transparency for AI systems and integrate structured public engagement in making of AI plan and regulation.

5. *Surveillance and Human Rights Concerns*

The increasing use of AI surveillance technology in regulating public life scenes has raised serious apprehensions among various groups about issues of privacy, freedom of expression, and human rights around the globe. Traditional AI instruments by governments to protect public safety will trigger new governance challenges, chiefly balancing security concerns against civil liberties. Use of AI-supported surveillance platforms such as the Automated Facial Recognition System (AFRS) plus Crime and Criminal Tracking Network System (CCTNS) has increased in India now. These operate in near-complete absence of law, data protection legislation, and human rights law in place. DPDPA 2023, while, in some aspect, protecting data privacy, provides limited safeguard against state surveillance and neither demands judicial approval nor public disclosure of any facial recognition deployments. Therefore, in the absence of independent regulatory bodies to audit or contest such activities, these measures jeopardize mass surveillance.

AI-based surveillance is heavily regulated in the European Union, thanks to relationship between GDPR and proposed AI Act of 2021. The AI Act recognizes real-time remote personal identification systems (like facelike recognition) in public places as high risk and generally unacceptable to the point of outright bans or serious restrictions. The EU also demands minimization of data, transparency, and independent oversight — all reinforcing its commitment to protection of fundamental rights, such as privacy and freedom of peaceful assembly. Within the European Union, AI-based surveillance is heavily regulated under both the GDPR with proposed AI Act (2021).

According to the AI Act, real time remote personal identification systems (like facial recognition) deployed in public places are "high-risk" and, in some cases, "unacceptable," which might lead to restrictions or outright prohibition. Echoing its commitment to protecting fundamental rights like privacy and freedom of assembly, the EU also demands openness, independent monitoring, and data minimization. In the US, there isn't a single government policy that deals with AI surveillance. However, other states and localities, such as Boston and San Francisco, have banned or suspended government facial recognition technology. Meanwhile, sometimes without enough openness, government agencies continue to use AI techniqu es for national security, immigration control, and predictive policing. The Blueprint for an AI Bill of Rights (2022) acknowledges potential dangers concerning AI surveillance together with suggests protections, but these are voluntary guidelines without binding legal authority.

China is the largest application of AI surveillance globally. With its Social Credit System and widespread facial recognition infrastructure, China has used AI to track public conduct, trace movements, and impose political obedience. International controversy has been raised against these tactics for violating minority rights, privacy, and freedom of expression, especially in Xinjiang. Chinese law prioritizes state security and does not include constitutional protections that are equal to those found in Western democracies to prevent the misuse of surveillance.

Japan is more reserved. Although AI is applied in public security, Japan does not engage in mass surveillance, and there is a robust cultural and legal focus on individual privacy. Surveillance activities are governed by data protection legislation, and AI uses in policing are usually pilot-scale and small, reflecting public concern about state overreach.

Canada has also shown concern regarding the utilization of AI for surveillance. Canada's Office of Privacy Commissioner has criticized the police's use of facial detection technology, citing

privacy law infringements and a failure to consult with the public. The newly proposed AIDA contains impact assessment requirements, particularly for higher-risk uses such as surveillance. This demonstrates Canada attempting to harmonize AI regulation with its Charter of Rights and Freedoms.

In short, India and China are confronted with the danger of untrammelled surveillance because of lax or non-existent legal checks, while the EU and Canada have more robust brakes on AI abuse. The US is a mixed bag, with differing protections by jurisdiction, and Japan is cautious in using AI surveillance. In order to support democratic values, India needs to establish constitutional checks, judicial control, and independent audit bodies for every AI-based surveillance effort.

6. ***Institutional Capacity***

Institutional capacity is the capacity of a nation's legal, regulatory, and administrative frameworks to design, implement, monitor, and enforce AI governance frameworks effectively. This involves the existence of competent regulatory institutions, technical knowledge, cross-sectoral coordination, and access to adequate resources. India is still in the initial phase of establishing institutional infrastructure for AI governance. Though NITI Aayog has been a catalytic force in defining India's AI vision through its #AIforAll initiative, there is no specific AI regulatory body or specialized public institution that monitors ethical, legal, or technical compliance. Sectoral regulators such as the Telecom Regulatory Authority of India (TRAI) or SEBI might cross paths with AI in their respective areas, but do not have uniform AI-specific guidelines. India also faces challenges related to limited public funding, low AI literacy among policymakers, and insufficient interdisciplinary collaboration between legal, technical, and ethical domains.

Conversely, the EU has strong institutional capability for AI regulation. European Data Protection Board (EDPB) as well as newly mooted European AI Office under the AI Act are required to impose compliance, issue guidance, and perform risk assessment. The EU is also strengthened by effective coordination among member states, wide public consultations, and expert committees, bringing together technical, legal, and ethical expertise to decision-making.

The US has a dispersed but asset-laden institutional framework. Institutions like the FTC, FDA, NIST, and Department of Defense all regulate various aspects of AI governance. Although there is no single AI authority, the OSTP and AI Research Resource Task Force are obligated for creating domestic standards and coordinating research on AI. There is also a robust academic and private sector ecosystem in the US, providing extensive institutional support for compliance and innovation.

China has developed a wide institutional apparatus with a state-centered AI governance orientation, propelled by organizations like Cyberspace Administration of China (CAC) and Ministry of Industry and Information Technology (MIIT). These institutions create binding regulations, perform audits, and set directions for the advancement of AI in a way that aligns with national objectives. China's institutional capability is extremely centralized, effective in application, yet absent of transparency, autonomous monitoring, and participation of civil society, which negates accountability.

Japan's institutional capability is decentralized and largely voluntary, with Ministry of Internal Affairs and Communications (MIC) along with Cabinet Office issuing guidelines. Japan's AI governance depends on industry standard-setting and self-regulation with support from public

research institutions and partnerships with academia. Although Japan advocates human-centered AI and ethics, institutional capacity is constrained by the lack of enforcement or a centralized AI regulator.

Canada is building its institutions of AI regulation gradually, with institutions like the Office of the Privacy Commissioner (OPC), also Innovation, Science and Economic Development Canada (ISED) playing a central role. The AIDA, which is being proposed, will give regulators the power to track compliance, impose fines, and undertake impact assessments. Canada's institutional strategy is centered on transparency, inclusiveness, and rights-oriented governance, supported by an expanding coalition of academic and civil society players engaged in AI policy-making.

In conclusion, the EU and Canada have high institutional preparedness with coordinated regulation and stakeholder involvement. The US has powerful sectoral institutions, although its absence of central coordination is a problem. China's centralized system is effective but does not have independent checks. Japan encourages ethical self-regulation with a moderate level of institutional infrastructure. India is in the process of developing basic institutional capacity and needs to invest in training, materials, and regulatory infrastructure in order to catch up with international developments.

6. POLICY RECOMMENDATIONS FOR INDIA

AI is growing across vital sectors in India, it is more important than ever that legal and policy structures adapt to guarantee ethical deployment, accountability, and safeguarding of basic rights. Informed by the comparative study of global frameworks and existing domestic issues, the following are recommended:

1. Passage of a Specific AI Regulation Act

India has to graduate beyond policy-level considerations and pass a holistic, rights-based AI Regulation Act. It should adopt risk-based supervisory structures**,** similar to EU AI Act, by classifying AI systems relying on adverse effect they put to public interest, safety, and core rights. Law should also explicitly regulate sensitive domains like facial recognition**,** biometric monitoring**,** and autonomous decision-making in public functions**,** ensuring safeguards are legally enforceable.

2. Formation *of a National AI Ethics and Compliance Authority*

To monitor ethical use of AI, there should be a creation of a National AI Ethics and Compliance Authority. This authority would operate independently, similar to the Data Protection Board, and should have the authority to:

- Issue binding ethical guidance
- Oversee compliance of AI systems
- Carry out investigations into malicious or discriminatory algorithms
- Offer sector-specific ethical regulation
- Enabling public consultation and feedback

Such an institutional mechanism would guarantee transparency, promote accountability, and serve as a redressal and stakeholder interaction forum**.**

3. Regular Algorithmic Audits of High-Risk AI Systems

Sensitive AI application—particularly those involved in criminal justice**,** healthcare**,** financial services, and employment—must undergo mandatory algorithmic audits**.** These audits should assess:

- Fairness and non-discrimination

- Accuracy and reliability
- Bias mitigation and transparency

Audits must be carried out by independent, certified third-party agencies at regular intervals, with enforceable standards and consequences for non-compliance.

4. **Liability and Accountability Legal Frameworks**

India should develop a clear legal framework for AI liability**,** determining who is accountable in cases where AI causes harm—be it the developer, deployer, or data controller. Drawing inspiration from product liability models and strict liability doctrines, the law must clarify:

- Definitions of negligence**,** intention**,** and causality in AI contexts
- Legal remedies for affected individuals
- Duties of care for AI designers and users

5. **Enhancing Privacy and Anti-Discrimination Guards**

While the DPDPA, 2023 lays the groundwork, AI-specific safeguards are essential. The following should be embedded into the legal framework:

- Protection from automated profiling and opaque algorithmic decisions
- The right to human intervention in high-risk AI outcomes
- Prohibition of algorithmic unfair treatment based on gender, caste, religion, or socio-economic status.
- Strict regulation of facial recognition and biometric data usage

These protections must be legally enforceable, with civil and criminal remedies where necessary.

6. **Promoting Responsible Innovation through Regulatory Sandboxes**

To balance regulation and innovation, India should scale up regulatory sandboxes under MeitY and relevant sectoral regulators. These controlled environments will allow:

- Startups and innovators to test AI applications under real-world conditions
- Regulators to observe risks and impacts in real time

This approach fosters collaborative learning, encourages responsible experimentation, and ensures ethical deployment without stifling growth.

7. CONCLUSION

This research has reviewed emerging context of AI regulation using a comparison between the international regime and India. As legal mechanism regulating AI is having different philosophies starting from risk based laws of EU, to innovation strategies in US, and state-centric management of China provided that it is important to have legal and ethical norms to handle AI related threat is crucial. Even though there are many challenges against AI reliability India is lacking to provide secure legal framework.

Through this research it is suggested importance of preparing an outline having the rules that strictly provides protection against the risks in the form online frauds, deepfaking, revenge porn etc. so that it also helps to encourage innovations in the various field. Moreover it is observed that AI system is having no boundaries, so it is necessary that all countries in the world come together and provide harmonized regulation. It requires cooperation, so as together we deal with the cross boarder threats providing ethical guidelines.

In conclusion, for India to harness the full promise of AI responsibly and equitably, it must formulate a visionary, inclusive, and rights-based legal architecture. This framework should be inspired by universal best practices, yet tailored to India's unique socio-economic realities. It must

address current gaps, offer legal certainty, and remain flexible enough to adapt to future technological advancements, ensuring that positive outcomes of AI are widely shared while its possible harms are effectively contained.

Reference :

1. European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*. Retrieved from https://eur-lex.europa.eu/.
2. European Parliament & Council. (2016). *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679.
3. High-Level Expert Group on AI. (2019). *Ethics Guidelines for Trustworthy AI*. European Commission.
4. Federal Trade Commission. (2021). *Aiming for truth, fairness, and equity in your company's use of AI*. Retrieved from https://www.ftc.gov.
5. State Council of China. (2017). *New Generation Artificial Intelligence Development Plan*. Retrieved from http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm
6. Cyberspace Administration of China. (2022). *Provisions on the Administration of Algorithmic Recommendation Services*.Retrieved fromhttps://www.cac.gov.cn.
7. Mozur, P. (2018). Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras. *The New York Times*. https://www.nytimes.com
8. Ministry of Internal Affairs and Communications. (2019). *AI Governance Guidelines*. https://www.soumu.go.jp.
9. Cabinet Office of Japan. (2020). *Society 5.0 – Realizing a super-smart society*, Retrieved from https://www8.cao.go.jp/cstp/english/society5_0/index.html
10. OECD. (2019). *OECD Principles on Artificial Intelligence*. https://www.oecd.org/going-digital/ai/principles/.
11. CIFAR. (2017). *Pan-Canadian Artificial Intelligence Strategy*. Canadian Institute for Advanced Research. https://cifar.ca/ai/pan-canadian-artificial-intelligence-strategy/
12. Government of Canada. (2022). *Bill C-27: Digital Charter Implementation Act, 2022*. Innovation, Science and Economic Development Canada. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html.
13. Treasury Board of Canada Secretariat. (2019). *Directive on Automated Decision-Making*. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.
14. NITI Aayog. (2018). *National Strategy for Artificial Intelligence #AIforAll*. Government of India. https://www.niti.gov.in/
15. Ministry of Law and Justice. (2023). *The Digital Personal Data Protection Act, 2023*. Government of India. https://www.meity.gov.in/
16. Baxi, A. (2020). How AI is transforming healthcare in India. *Forbes India*. https://www.forbesindia.com

17. Indian Council of Agricultural Research. (2021). *AI and Robotics in Agriculture*. Government of India.
18. Reserve Bank of India. (2021). *Report on Digital Lending Including Lending through Online Platforms and Mobile Apps*. https://rbi.org.in
19. National Crime Records Bureau. (2020). *Request for Proposal: AFRS System*. Ministry of Home Affairs, India.
20. Ministry of Home Affairs. (2019). *CCTNS and ICJS Implementation Status*. Government of India. https://www.mha.gov.in/