



Technology and Artificial Intelligence Law in India: A Critical Analysis of Legal Challenges, Regulatory Framework and Emerging Jurisprudence

Author: **K Jagadish**

Affiliation: Aurora University, Second Year LL.B.

Date: September 2026

A LAW JOURNAL

How to Cite this Article:

Jagadish, K. (2026). Technology and Artificial Intelligence Law in India: A Critical Analysis of Legal Challenges, Regulatory Framework and Emerging Jurisprudence. International Journal of Creative and Open Research in Engineering and Management, 2(10), 1-9.
<https://doi.org/10.55041/ijcope.v2i10.040>

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.



<https://doi.org/10.55041/ijcope.v2i10.040>

ABSTRACT

Technology has become an essential part of modern society, influencing almost every aspect of human life, including communication, commerce, healthcare, education, banking, governance and the administration of justice. Among the most significant technological developments of the twenty-first century is Artificial Intelligence (AI). Artificial Intelligence refers to computer systems capable of performing tasks that traditionally require human intelligence, such as learning, reasoning, prediction, decision-making, language processing and image recognition.

The rapid development of AI presents considerable opportunities for economic and social development, but it also creates complex legal and ethical challenges. Questions relating to privacy, data protection, discrimination, algorithmic bias, intellectual property rights, cybercrime, intermediary liability, consumer protection, employment, surveillance, deepfakes, autonomous systems and accountability have become increasingly important.

India does not presently have a single comprehensive legislation exclusively regulating Artificial Intelligence. Instead, the legal framework is distributed among constitutional principles, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, intellectual property legislation, criminal law,

consumer protection law, contract law and sector-specific regulations. Government policy initiatives, including the National Strategy for Artificial Intelligence and the Responsible AI framework developed by NITI Aayog, have also contributed to India's emerging AI governance framework.

The Supreme Court of India has developed important constitutional principles concerning privacy, freedom of speech, informational autonomy and technological governance. Decisions such as *Justice K.S. Puttaswamy (Retd.) v Union of India*, *Shreya Singhal v Union of India*, *Anuradha Bhasin v Union of India* and *Justice K.S. Puttaswamy (Retd.) v Union of India (Aadhaar)* provide a constitutional foundation for addressing several AI-related concerns. However, specifically AI-generated content, AI authorship, algorithmic decision-making and liability for autonomous systems remain comparatively underdeveloped areas of Indian jurisprudence.

This paper critically examines the existing Indian legal framework governing technology and Artificial Intelligence. It analyses constitutional rights, data protection, cyber law, intellectual property, intermediary liability, AI-generated content, deepfakes, algorithmic discrimination and emerging jurisprudence. It further compares selected international approaches and proposes a balanced Indian regulatory model based upon innovation, transparency, accountability, human oversight and protection of fundamental rights.



Keywords: Artificial Intelligence, Technology Law, AI Governance, Data Protection, Privacy, Algorithmic Bias, Cyber Law, Deepfakes, Intellectual Property, Digital Personal Data, Constitutional Law, Intermediary Liability.

TABLE OF CONTENTS

1. Introduction
2. Concept and Evolution of Artificial Intelligence
3. Constitutional Framework Governing Technology and AI in India
4. Indian Legal and Regulatory Framework
5. Artificial Intelligence and Data Protection
6. Artificial Intelligence, Intellectual Property and Copyright
7. AI, Cybercrime, Deepfakes and Online Harms
8. Algorithmic Bias, Discrimination and Human Rights
9. Liability and Accountability for AI Systems
10. Emerging Indian and International Jurisprudence
11. Comparative Legal Approaches
12. Challenges in Regulating Artificial Intelligence in India
13. Recommendations and Future Legal Framework
14. Conclusion
15. Table of Cases
16. Bibliography
17. Online Resources

LIST OF ABBREVIATIONS

Abbreviation Meaning

AI	Artificial Intelligence
AGI	Artificial General Intelligence
ANI	Artificial Narrow Intelligence
BNS	Bharatiya Nyaya Sanhita, 2023
BNSS	Bharatiya Nagarik Suraksha Sanhita, 2023
BSA	Bharatiya Sakshya Adhinyam, 2023
CERT-In	Indian Computer Emergency Response Team
CJI	Chief Justice of India
DPDP Act	Digital Personal Data Protection Act, 2023
EU	European Union
GDPR	General Data Protection Regulation
IPR	Intellectual Property Rights
IT Act	Information Technology Act, 2000
IT Rules	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
ML	Machine Learning
NLP	Natural Language Processing
OECD	Organisation for Economic Co-operation and Development
RBI	Reserve Bank of India
SCC	Supreme Court Cases
SEBI	Securities and Exchange Board of India
UN	United Nations



UNESCO	United Nations Educational, Scientific and Cultural Organization
UIDAI	Unique Identification Authority of India
VLSI	Very Large-Scale Integration

CHAPTER 1

INTRODUCTION

1.1 Background

The development of technology has fundamentally changed the relationship between individuals, businesses and the State. The internet, smartphones, cloud computing, big data and social media have created an interconnected digital environment.

Artificial Intelligence represents the next major stage of technological development. Unlike traditional computer programs, many modern AI systems can process large amounts of information, identify patterns and produce outputs without direct human instructions for every individual task.

AI is now used in:

- healthcare;
- banking and finance;
- education;
- employment;
- policing;
- transportation;
- e-commerce;
- advertising;
- content creation;
- judicial research;
- national security; and
- public administration.

The increasing use of AI has created an important legal question:

Who should be legally responsible when an AI system causes harm?

Other questions include:

- Who owns AI-generated content?
- Can an AI system be considered an inventor?
- Can personal data be used to train AI?
- Who is responsible for discriminatory algorithmic decisions?
- Should individuals have a right to know how an important AI decision was made?
- How should deepfakes be regulated?
- Can AI-generated defamatory content result in legal liability?
- Should developers, deployers or users be responsible for AI-related harm?

These questions demonstrate that AI is not merely a technological issue. It is increasingly a matter of constitutional law, criminal law, civil law, intellectual property law, data protection law and human rights.



1.2 Statement of the Problem

India currently does not have one comprehensive AI statute dealing with all applications of Artificial Intelligence. Instead, different legal provisions may apply depending upon the nature of the activity.

For example:

- privacy issues may involve constitutional law and the DPDP Act;
- cyber offences may involve the IT Act and criminal law;
- copyright issues may involve the Copyright Act, 1957;
- patent issues may involve the Patents Act, 1970;
- consumer harm may involve the Consumer Protection Act, 2019;
- intermediary issues may involve the IT Act and IT Rules;
- financial AI applications may involve RBI or SEBI regulations.

This fragmented framework creates uncertainty concerning responsibility and enforcement.

1.3 Objectives of the Study

The major objectives are:

1. To examine the concept and development of Artificial Intelligence.
2. To analyse the constitutional framework applicable to AI in India.
3. To examine existing Indian technology and cyber laws.
4. To analyse the Digital Personal Data Protection Act, 2023 in relation to AI.
5. To study AI-related intellectual property issues.
6. To examine deepfakes and AI-enabled cybercrime.
7. To analyse algorithmic bias and discrimination.
8. To examine liability and accountability for AI-related harm.
9. To analyse important Indian and foreign judicial decisions.
10. To identify gaps in India's existing regulatory framework.
11. To recommend a balanced legal framework for responsible AI governance.

1.4 Research Questions

The study addresses the following questions:

1. Is India's existing legal framework sufficient to regulate Artificial Intelligence?
2. How does the constitutional right to privacy apply to AI systems?
3. Who owns AI-generated works under Indian copyright law?
4. How should liability be determined when AI causes harm?
5. How should deepfakes and AI-generated misinformation be regulated?
6. How can algorithmic discrimination be prevented?
7. Should India enact a dedicated Artificial Intelligence law?
8. What lessons can India learn from the EU and other jurisdictions?

1.5 Research Methodology

The research adopts a doctrinal legal research methodology.

The study relies upon:

- legislation;
- constitutional provisions;



- judicial decisions;
- government reports;
- policy documents;
- books;
- journal articles;
- international instruments; and
- credible online legal resources.

The research is primarily analytical and comparative in nature.

CHAPTER 2

CONCEPT AND EVOLUTION OF ARTIFICIAL INTELLIGENCE

2.1 Meaning of Artificial Intelligence

Artificial Intelligence can broadly be described as the ability of a machine or computer system to perform tasks associated with human intelligence.

These tasks may include:

- learning;
- reasoning;
- problem-solving;
- perception;
- language understanding;
- prediction; and
- decision-making.

AI should not necessarily be understood as a machine possessing human consciousness. Most current AI systems are specialised systems designed for particular tasks.

2.2 Types of AI

A. Narrow AI

Narrow AI is designed to perform a particular task.

Examples include:

- facial recognition;
- recommendation systems;
- spam filters;
- voice assistants;
- fraud detection.

B. General AI

Artificial General Intelligence refers to a theoretical system capable of performing a broad range of intellectual tasks comparable to human intelligence.

General AI has not yet become an established practical technology.



C. Generative AI

Generative AI creates new content based on patterns learned from existing data.

It can generate:

- text;
- images;
- audio;
- video;
- software code; and
- other forms of digital content.

Examples include large language models and image-generation systems.

2.3 Machine Learning

Machine Learning is a major branch of AI.

Instead of programming every individual instruction, machine-learning systems identify patterns from data.

This creates legal concerns because decisions may be influenced by training data that contain errors or historical discrimination.

2.4 Deep Learning

Deep Learning uses artificial neural networks with multiple layers to process complex data.

It is extensively used in:

- computer vision;
- speech recognition;
- natural language processing;
- autonomous systems; and
- generative AI.

2.5 Benefits of AI

AI can contribute to:

- faster medical diagnosis;
- improved agricultural productivity;
- fraud detection;
- efficient public administration;
- legal research;
- personalised education;
- accessibility for persons with disabilities;
- scientific research; and
- economic growth.

However, these benefits must be balanced against legal and social risks.



CHAPTER 3

CONSTITUTIONAL FRAMEWORK GOVERNING TECHNOLOGY AND AI IN INDIA

The Indian Constitution does not expressly mention Artificial Intelligence. Nevertheless, existing fundamental rights provide an important framework for regulating AI.

3.1 Article 14 – Equality Before Law

Article 14 guarantees equality before law and equal protection of laws.

AI systems may create Article 14 concerns when automated decision-making produces arbitrary or discriminatory outcomes.

For example, if an AI recruitment system consistently rejects applicants belonging to a particular group because of biased training data, the issue may raise equality concerns.

3.2 Article 19(1)(a) – Freedom of Speech and Expression

Digital platforms have become important spaces for expression.

AI creates both opportunities and threats for freedom of expression.

Generative AI can facilitate creative expression, but AI-generated misinformation, impersonation and manipulated media may cause serious harm.

Regulation must therefore balance:

freedom of expression + prevention of genuine harm.

3.3 Article 21 – Right to Life and Personal Liberty

Article 21 has been interpreted broadly by the Supreme Court.

It encompasses several rights relating to dignity, autonomy and privacy.

The most important case in this context is:

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

A nine-judge Constitution Bench recognised privacy as a fundamental right protected by the Constitution.

The judgment is extremely important for AI because modern AI systems depend heavily upon data.

AI-related privacy concerns may include:

- surveillance;
- facial recognition;
- profiling;
- behavioural prediction;
- location tracking;
- biometric processing; and
- automated profiling.



3.4 Informational Privacy

Informational privacy is particularly important in AI governance.

AI systems may process information concerning:

- identity;
- health;
- financial transactions;
- location;
- preferences;
- online behaviour; and
- biometric characteristics.

The principle of informational autonomy requires individuals to have meaningful protection against misuse of personal information.

3.5 *K.S. Puttaswamy (Aadhaar) v Union of India*

In *K.S. Puttaswamy (Retd.) v Union of India*, (2019) 1 SCC 1, the Supreme Court considered issues concerning Aadhaar, privacy and proportionality.

The decision demonstrates the importance of:

- legality;
- legitimate State purpose;
- proportionality; and
- protection against excessive intrusion.

These principles can provide guidance when evaluating government use of AI.

3.6 Article 19 and Algorithmic Transparency

Where government authorities use AI to make decisions affecting citizens, individuals may argue that opaque decision-making can affect procedural fairness and constitutional rights.

A significant future issue is whether a person should have a right to obtain an explanation when an important governmental decision is substantially influenced by an algorithm.

CHAPTER 4

INDIAN LEGAL AND REGULATORY FRAMEWORK

India regulates technology through several statutes rather than a single comprehensive technology law.

4.1 Information Technology Act, 2000

The Information Technology Act, 2000 is India's principal cyber law.

It addresses matters including:

- electronic records;
- electronic signatures;
- cyber offences;



- unauthorised access;
- identity theft;
- cheating by personation using computer resources;
- privacy-related offences; and
- intermediary liability.

Several provisions are relevant to AI-enabled misconduct.

4.2 Section 43 – Unauthorised Access and Damage

Section 43 provides civil consequences for various unauthorised acts involving computer systems.

AI-enabled cyberattacks may involve:

- unauthorised access;
- data extraction;
- introduction of malicious code;
- disruption of systems.

4.3 Section 66 – Computer-Related Offences

Where acts contemplated by Section 43 are done dishonestly or fraudulently, Section 66 may become relevant.

AI can increase the scale and sophistication of cyber offences.

4.4 Section 66C – Identity Theft

AI can be used to impersonate individuals through:

- stolen credentials;
- synthetic identities;
- voice cloning;
- facial manipulation.

Section 66C may become relevant depending on the circumstances.

4.5 Section 66D – Cheating by Personation

AI-generated voice and video can facilitate impersonation scams.

For example, criminals may create a synthetic voice resembling a family member and demand money from relatives.

Such conduct may potentially attract Section 66D along with other applicable laws.

4.6 Section 79 – Intermediary Liability

Section 79 establishes a safe-harbour framework for intermediaries subject to specified conditions.

The growth of AI-generated content raises questions concerning:

- content moderation;
- notice and takedown;
- platform responsibility;



- synthetic media;
- deepfakes; and
- recommender systems.

4.7 Information Technology Rules, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 establish due-diligence obligations for intermediaries.

They are important in addressing harmful online content.

AI-generated misinformation and deepfakes make intermediary governance increasingly significant.

CHAPTER 5

ARTIFICIAL INTELLIGENCE AND DATA PROTECTION

5.1 Importance of Data in AI

Data is the fundamental resource upon which many AI systems operate.

An AI model may require enormous datasets for:

- training;
- validation;
- testing; and
- improvement.

Where datasets contain personal information, data protection law becomes relevant.

5.2 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 represents an important development in India's privacy and data governance framework.

The Act establishes a framework concerning processing of digital personal data.

Key concepts include:

- Data Principal;
- Data Fiduciary;
- Data Processor;
- consent;
- certain legitimate uses;
- obligations of Data Fiduciaries;
- security safeguards;
- breach-related obligations;
- rights of Data Principals; and
- penalties.



5.3 AI Training and Personal Data

A major issue is whether personal data can lawfully be used to train AI models.

Consider an AI company collecting millions of publicly accessible documents containing names, photographs and personal information.

The fact that information is publicly available does not automatically resolve every question concerning lawful processing.

Questions include:

1. What is the purpose of processing?
2. Is there a lawful basis?
3. Is the processing proportionate?
4. Are individuals adequately informed?
5. Is the data necessary?
6. How long will the information be retained?

5.4 Automated Decision-Making

AI may be used to make or assist decisions concerning:

- employment;
- credit;
- insurance;
- education;
- healthcare;
- public benefits.

The greater the effect on an individual's rights, the stronger the argument for transparency, human oversight and procedural safeguards.

5.5 Data Security

AI databases can become attractive targets for cybercriminals.

Data breaches may expose:

- personal information;
- financial information;
- medical records;
- biometric information; and
- confidential business data.

Therefore, organisations deploying AI must adopt appropriate security measures.

CHAPTER 6

ARTIFICIAL INTELLIGENCE, INTELLECTUAL PROPERTY AND COPYRIGHT

AI presents difficult questions for intellectual property law.



6.1 Copyright and AI-Generated Works

Under traditional copyright principles, copyright protects original works created through human authorship.

Generative AI complicates this principle.

Suppose a person enters a prompt into an AI system and receives an image.

Who is the author?

Possible answers include:

1. the user;
2. the AI developer;
3. the person who selected or edited the output;
4. nobody, where sufficient human authorship is absent.

Indian copyright law does not presently provide a comprehensive statutory answer to every such scenario.

6.2 Copyright Act, 1957

The Copyright Act, 1957 remains the principal Indian copyright statute.

Section 13 deals with works in which copyright subsists.

Section 17 deals with first ownership.

The statutory framework was developed before modern generative AI and therefore creates interpretative challenges.

6.3 Originality

Eastern Book Company v D.B. Modak, (2008) 1 SCC 1

The Supreme Court discussed originality in Indian copyright law and rejected a purely mechanical approach.

The requirement of originality becomes relevant to AI-generated works because courts may need to determine the extent of human intellectual contribution.

6.4 AI as an Inventor

Patent law creates another major issue.

Can an AI system itself be named as an inventor?

Thaler v Comptroller-General of Patents, Designs and Trade Marks [2021] UKSC 49

The United Kingdom Supreme Court held that under the relevant statutory framework, an inventor must be a natural person.

The case concerned the DABUS AI system.

The decision illustrates the difficulty of applying traditional patent concepts to autonomous AI systems.



6.5 United States – AI Copyright

Thaler v Perlmutter, 687 F. Supp. 3d 140 (D.D.C. 2023)

The United States District Court for the District of Columbia held that copyright protection requires human authorship.

Although foreign decisions are not binding in India, they provide useful comparative material.

6.6 Training Data and Copyright

Another major issue is whether copyrighted works can lawfully be used for training AI models.

Possible legal concerns include:

- reproduction;
- adaptation;
- substantial similarity;
- licensing;
- fair dealing;
- database rights in jurisdictions where recognised; and
- commercial exploitation.

Indian courts may eventually be required to determine the relationship between AI training and copyright infringement.

CHAPTER 7

AI, CYBERCRIME, DEEPFAKES AND ONLINE HARMS

7.1 Meaning of Deepfake

A deepfake is synthetic or manipulated audio, image or video that can make it appear that a person said or did something that did not actually happen.

Deepfakes may be created using AI and machine-learning techniques.

7.2 Legal Risks of Deepfakes

Deepfakes can result in:

- defamation;
- identity theft;
- fraud;
- harassment;
- privacy violations;
- sexual exploitation;
- misinformation;
- election-related manipulation; and
- reputational damage.



7.3 Deepfakes and Defamation

Indian defamation law can potentially apply where false statements cause reputational harm.

Depending upon the circumstances, criminal and civil remedies may be available.

The challenge is attribution.

The victim may not know:

- who created the deepfake;
- who uploaded it;
- who distributed it; or
- which platform first hosted it.

7.4 Deepfakes and Women

AI-generated non-consensual intimate imagery represents a particularly serious concern.

The harm can involve:

- loss of dignity;
- psychological distress;
- reputational injury;
- harassment;
- sexual exploitation.

Existing criminal and cyber laws may apply, but enforcement remains difficult.

7.5 AI and Cyber Fraud

AI can make traditional fraud more convincing.

For example:

A fraudster may use voice-cloning technology to imitate a company director and instruct an employee to transfer funds.

The existing criminal law framework can potentially address the underlying fraudulent conduct, but evidentiary and attribution challenges may arise.

CHAPTER 8

ALGORITHMIC BIAS, DISCRIMINATION AND HUMAN RIGHTS

8.1 Meaning of Algorithmic Bias

Algorithmic bias occurs when an AI system produces systematically unfair or discriminatory outcomes.

Bias can originate from:

- training data;
- data collection;
- model design;



- assumptions made by developers;
- incomplete datasets; or
- human decisions surrounding deployment.

8.2 Example of Recruitment Bias

Suppose an AI recruitment system is trained using historical recruitment data.

If historical hiring practices disproportionately preferred one group, the AI system may learn that pattern.

The system may therefore reproduce historical discrimination.

This creates a fundamental legal question:

Can an organisation avoid liability by arguing that the discriminatory decision was made by an algorithm?

The answer should not simply be yes.

8.3 Article 14 and Algorithmic Fairness

AI systems used by public authorities must comply with constitutional principles.

An automated decision should not become immune from judicial review merely because it was produced by a computer.

8.4 Right to Human Oversight

For high-impact decisions, human oversight is essential.

Examples include:

- denial of healthcare;
- criminal justice decisions;
- immigration;
- employment;
- credit;
- welfare benefits.

AI should assist human decision-making rather than eliminate accountability.

8.5 Explainability

AI systems may sometimes operate as "black boxes".

The person affected may receive an outcome without understanding why the system reached it.

This creates concerns regarding:

- natural justice;
- procedural fairness;
- accountability;
- transparency; and
- judicial review.



CHAPTER 9

LIABILITY AND ACCOUNTABILITY FOR AI SYSTEMS

One of the most difficult questions in AI law concerns liability.

9.1 Who Should Be Liable?

Potentially responsible parties include:

1. AI developer;
2. manufacturer;
3. data provider;
4. deployer;
5. business using AI;
6. platform;
7. end user.

The appropriate party may depend upon the circumstances.

9.2 Product Liability

Where an AI-enabled product causes physical or financial harm, product liability principles may become relevant.

The Consumer Protection Act, 2019 provides a framework concerning product liability in specified circumstances.

9.3 Negligence

Traditional negligence requires consideration of:

- duty of care;
- breach;
- causation; and
- damage.

AI systems make causation more complicated.

If an autonomous system makes an unexpected decision, courts may need to determine whether the harm resulted from:

- defective design;
- inadequate testing;
- poor training data;
- negligent deployment;
- insufficient human supervision; or
- unforeseeable system behaviour.

9.4 Strict Liability

There may be arguments for stricter liability in certain high-risk AI applications.

However, excessive liability may discourage innovation.



The law must therefore balance:

innovation + accountability + consumer protection.

9.5 Human Accountability

AI should not be treated as a legal person merely because it can make sophisticated decisions.

A machine does not possess the same legal personality, consciousness or moral responsibility as a human being.

Therefore, responsibility should generally remain traceable to human or corporate actors.

CHAPTER 10

EMERGING INDIAN AND INTERNATIONAL JURISPRUDENCE

Indian AI jurisprudence is still developing. However, existing constitutional and technology cases provide important principles.

10.1 *Shreya Singhal v Union of India*

***Shreya Singhal v Union of India*, (2015) 5 SCC 1**

The Supreme Court struck down Section 66A of the Information Technology Act, 2000.

The judgment strongly protected freedom of speech and expression online.

Relevance to AI

The decision demonstrates that technology regulation must comply with constitutional guarantees.

AI-generated speech and online content should therefore be regulated in a manner consistent with Article 19(1)(a).

10.2 *Anuradha Bhasin v Union of India*

***Anuradha Bhasin v Union of India*, (2020) 3 SCC 637**

The Supreme Court considered restrictions on internet access and emphasised constitutional principles concerning freedom of speech and expression.

Relevance

The judgment establishes that constitutional rights do not disappear merely because they are exercised through technology.

10.3 *Justice K.S. Puttaswamy v Union of India*

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

The recognition of privacy as a fundamental right is foundational for AI regulation.



AI systems capable of extensive profiling and surveillance must be assessed against privacy and dignity principles.

10.4 Justice K.S. Puttaswamy v Union of India (Aadhaar)

K.S. Puttaswamy (Retd.) v Union of India, (2019) 1 SCC 1

The judgment provides significant discussion concerning privacy, proportionality and State use of personal data.

It is relevant to AI-based governmental databases and biometric systems.

10.5 Google India Pvt Ltd v Visaka Industries Ltd

The Supreme Court's intermediary-related jurisprudence is relevant to the question of platform responsibility.

AI-generated content creates new challenges concerning the boundaries of intermediary protection.

10.6 Christian Louboutin SAS v Nakul Bajaj

Christian Louboutin SAS v Nakul Bajaj, 2018 SCC OnLine Del 12987

The Delhi High Court considered the role of an intermediary and circumstances in which active participation may affect intermediary protection.

This reasoning can become relevant when platforms actively use algorithms to recommend, rank or distribute AI-generated content.

10.7 ANI Media Pvt Ltd v OpenAI

The litigation involving ANI Media and OpenAI represents an important emerging Indian dispute concerning generative AI, copyright and the use of copyrighted content.

The matter illustrates the developing legal debate over:

- AI training;
- copyrighted databases;
- content reproduction;
- licensing;
- AI outputs; and
- jurisdiction.

As the jurisprudence develops, it may become one of the important Indian authorities concerning generative AI and copyright.

10.8 Thaler v Comptroller-General

The UK Supreme Court's DABUS decision provides an important comparative authority concerning AI-generated inventions.

It demonstrates that traditional concepts such as "inventor" may require reconsideration in the age of AI.



10.9 Thaler v Perlmutter

The United States decision concerning an AI-generated artwork illustrates the continued importance of human authorship in copyright law.

CHAPTER 11

COMPARATIVE LEGAL APPROACHES

11.1 European Union

The European Union has adopted a risk-based approach through the **EU Artificial Intelligence Act**.

AI systems are classified according to their level of risk.

Broad categories include:

- prohibited AI practices;
- high-risk AI systems;
- transparency-related obligations; and
- obligations relating to certain general-purpose AI models.

The EU approach demonstrates a movement away from treating all AI systems identically.

11.2 United States

The United States has generally relied upon a combination of:

- existing laws;
- sector-specific regulation;
- executive action;
- agency enforcement; and
- state legislation.

This approach is comparatively decentralised.

11.3 United Kingdom

The UK has pursued a relatively flexible, principles-based approach.

The DABUS patent litigation demonstrates how existing intellectual property statutes are being applied to AI-related questions.

11.4 OECD AI Principles

The OECD AI Principles emphasise:

- inclusive growth;
- sustainable development;
- human-centred values;
- transparency;
- explainability;
- robustness;
- security; and



- accountability.

These principles provide useful guidance for Indian AI governance.

11.5 UNESCO Recommendation on the Ethics of Artificial Intelligence

UNESCO's Recommendation on the Ethics of Artificial Intelligence, adopted in 2021, emphasises:

- human rights;
- human dignity;
- fairness;
- transparency;
- accountability;
- environmental protection; and
- human oversight.

These principles are particularly relevant to responsible AI governance.

CHAPTER 12

CHALLENGES IN REGULATING ARTIFICIAL INTELLIGENCE IN INDIA

12.1 Absence of a Comprehensive AI Statute

India has no single comprehensive AI law covering all AI applications.

This may result in regulatory fragmentation.

12.2 Rapid Technological Development

Technology develops much faster than legislation.

A law designed for one technological generation may become outdated quickly.

12.3 Attribution of Liability

It may be difficult to identify the legally responsible actor where several parties contribute to an AI system.

12.4 Algorithmic Opacity

Many AI models are difficult to interpret.

This creates problems for:

- courts;
- regulators;
- affected individuals; and
- auditors.

12.5 Cross-Border AI Services

Many AI services are provided by companies located outside India.

This raises issues concerning:



- jurisdiction;
- enforcement;
- data transfers;
- applicable law; and
- international cooperation.

12.6 AI and Employment

Automation may change the nature of employment.

AI can:

- replace some tasks;
- create new employment;
- alter existing occupations; and
- increase demand for technical skills.

Indian labour law may need to adapt to these changes.

12.7 AI and Children

Children may be particularly vulnerable to:

- addictive recommendation systems;
- AI-generated misinformation;
- inappropriate content;
- profiling;
- exploitation; and
- manipulation.

Child-centred AI safeguards are therefore essential.

12.8 AI in Criminal Justice

AI may be used for:

- predictive policing;
- facial recognition;
- risk assessment;
- forensic analysis.

However, inaccurate or biased AI can result in serious consequences for individual liberty.

Human oversight and judicial safeguards are therefore essential.

CHAPTER 13

RECOMMENDATIONS AND FUTURE LEGAL FRAMEWORK

13.1 Adoption of a Risk-Based Regulatory Framework

India should consider a risk-based framework.

AI applications could be classified as:



Low Risk

Ordinary applications such as basic productivity tools.

Moderate Risk

Systems involving consumer profiling or recommendation.

High Risk

Healthcare, employment, credit, education, policing and critical infrastructure.

Prohibited or Unacceptable Risk

AI applications causing serious and unjustifiable violations of fundamental rights.

13.2 Mandatory Human Oversight

High-risk AI systems should have meaningful human oversight.

Humans should retain the authority to:

- review;
- override; and
- challenge AI decisions.

13.3 Algorithmic Impact Assessments

Organisations deploying high-risk AI should conduct an assessment of:

- privacy risks;
- discrimination;
- security;
- reliability;
- human rights;
- explainability.

13.4 AI Audit Mechanism

Independent audits should be encouraged or required for high-risk systems.

Audits may examine:

- accuracy;
- bias;
- security;
- explainability;
- data quality;
- compliance.

13.5 Deepfake Regulation

Platforms should develop effective mechanisms for:



- detection;
- labelling;
- reporting;
- rapid removal of unlawful content;
- preservation of evidence; and
- victim support.

However, regulation should not unnecessarily suppress legitimate satire, artistic expression or political speech.

13.6 Protection of Copyright

India should develop clearer rules regarding:

- AI training datasets;
- licensing;
- copyrighted inputs;
- AI-generated outputs;
- human authorship;
- attribution.

13.7 Right to Explanation

For high-impact decisions, affected persons should receive meaningful information concerning the principal reasons for an AI-assisted decision.

13.8 AI Regulatory Authority

India could consider a specialised regulatory mechanism or coordinated regulatory structure for high-risk AI.

However, a new regulator should avoid unnecessary duplication with existing institutions.

13.9 Promotion of AI Innovation

Regulation should not be designed solely around restrictions.

India should encourage:

- AI research;
- Indian-language AI;
- healthcare AI;
- agricultural AI;
- education technology;
- responsible start-ups;
- public-interest technology.

13.10 AI Literacy

Citizens should be educated about:

- deepfakes;
- online fraud;
- AI-generated misinformation;
- privacy;
- cybersecurity;



- responsible use of generative AI.

Legal education institutions should also introduce AI law as an emerging field.

CHAPTER 14

CONCLUSION

Artificial Intelligence is one of the most transformative technological developments of the modern era. It has the potential to improve healthcare, education, economic productivity, governance and scientific research. At the same time, uncontrolled or poorly governed AI can threaten privacy, equality, dignity, freedom of expression, intellectual property and individual autonomy.

India already possesses a substantial legal foundation for addressing many technology-related harms. The Constitution provides fundamental rights; the Information Technology Act regulates cyber activities; the Digital Personal Data Protection Act provides a framework for digital personal data; intellectual property laws protect creative and inventive works; consumer protection law addresses certain forms of consumer harm; and sectoral regulators provide additional oversight.

Nevertheless, these laws were largely developed before the widespread emergence of generative AI and autonomous decision-making systems. Consequently, significant questions remain unanswered.

The central objective of AI regulation should not be to stop technological innovation. Instead, the objective should be to ensure that innovation takes place within a framework of legality, accountability, transparency and respect for human dignity.

India should therefore adopt a balanced and risk-based approach. High-risk AI systems should be subject to stronger requirements concerning transparency, human oversight, security, accountability and impact assessment. At the same time, low-risk innovation should not be burdened by unnecessary regulation.

The future of AI law in India should ultimately be based upon the principle that **technology must remain subordinate to constitutional values and human rights**.

AI may make decisions, but legal responsibility should remain capable of being traced to human beings and institutions.

The development of Indian AI jurisprudence is only beginning. Courts, Parliament, regulators, academics and technology companies will collectively shape the future legal framework. The challenge is to create a system that protects citizens while allowing India to remain a leading participant in the global technological economy.

TABLE OF IMPORTANT CASES

Indian Cases

1. *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1.
2. *K.S. Puttaswamy (Retd.) v Union of India*, (2019) 1 SCC 1.
3. *Shreya Singhal v Union of India*, (2015) 5 SCC 1.
4. *Anuradha Bhasin v Union of India*, (2020) 3 SCC 637.
5. *R. Rajagopal v State of Tamil Nadu*, (1994) 6 SCC 632.
6. *People's Union for Civil Liberties v Union of India*, (1997) 1 SCC 301.
7. *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
8. *Eastern Book Company v D.B. Modak*, (2008) 1 SCC 1.



9. *R.G. Anand v Deluxe Films*, (1978) 4 SCC 118.
10. *Google India Pvt Ltd v Visaka Industries Ltd.*
11. *Christian Louboutin SAS v Nakul Bajaj*, 2018 SCC OnLine Del 12987.
12. *ANI Media Pvt Ltd v OpenAI Inc.*, Delhi High Court proceedings concerning generative AI and copyright.

Foreign Cases

13. *Thaler v Comptroller-General of Patents, Designs and Trade Marks* [2021] UKSC 49.
14. *Thaler v Perlmutter*, 687 F. Supp. 3d 140 (D.D.C. 2023).
15. *Authors Guild v Google, Inc.*, 804 F.3d 202 (2d Cir. 2015).

STATUTES AND PRIMARY LEGAL MATERIALS

1. Constitution of India, 1950.
2. Information Technology Act, 2000.
3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
4. Digital Personal Data Protection Act, 2023.
5. Copyright Act, 1957.
6. Patents Act, 1970.
7. Trade Marks Act, 1999.
8. Consumer Protection Act, 2019.
9. Indian Contract Act, 1872.
10. Bharatiya Nyaya Sanhita, 2023.
11. Bharatiya Nagarik Suraksha Sanhita, 2023.
12. Bharatiya Sakshya Adhinyam, 2023.
13. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
14. Digital Personal Data Protection Rules, as applicable.
15. EU Artificial Intelligence Act, Regulation (EU) 2024/1689.

BIBLIOGRAPHY

A. BOOKS

1. Pavan Duggal, *Artificial Intelligence Law*, Universal Law Publishing / relevant editions.
2. Pavan Duggal, *Cyber Law: The Indian Perspective*, Saakshar Law Publications.
3. Vakul Sharma, *Information Technology Law and Practice*, Universal Law Publishing.
4. Apar Gupta, *Internet Law: Regulating Cyberspace and Emerging Technologies*, LexisNexis / relevant edition.
5. S. K. Verma and Raman Mittal, *Intellectual Property Rights: Indian and Global Perspectives*, relevant edition.
6. N.S. Gopalakrishnan and T.G. Agitha, *Principles of Intellectual Property*, Eastern Book Company.
7. Richard Susskind, *Online Courts and the Future of Justice*, Oxford University Press, 2019.
8. Richard Susskind, *Tomorrow's Lawyers: An Introduction to Your Future*, Oxford University Press.
9. Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press, 2014.
10. Stuart Russell, *Human Compatible: Artificial Intelligence and the Problem of Control*, Viking, 2019.
11. Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown, 2016.
12. Shoshana Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, 2019.



13. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015.
14. Ryan Calo, *Robotics and the Lessons of Cyberlaw*, relevant academic materials.
15. Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books.

B. JOURNAL ARTICLES

1. Sandra Wachter, Brent Mittelstadt and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, Vol. 7, Issue 2, 2017.
2. Joshua A. Kroll et al., "Accountable Algorithms", *University of Pennsylvania Law Review*, Vol. 165, 2017.
3. Danielle Keats Citron and Frank Pasquale, "The Scored Society: Due Process for Automated Predictions", *Washington Law Review*, Vol. 89, 2014.
4. Andrew D. Selbst and Solon Barocas, "The Intuitive Appeal of Explainable Machines", *Fordham Law Review*, Vol. 87, 2018.
5. Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact", *California Law Review*, Vol. 104, 2016.
6. Danielle Keats Citron, "Technological Due Process", *Washington University Law Review*, Vol. 85, 2008.
7. Cary Coglianese and David Lehr, "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era", *Georgetown Law Journal*, Vol. 105, 2017.
8. Woodrow Hartzog, "Privacy's Blueprint: The Battle to Control the Design of New Technologies", relevant scholarship on privacy and technology.
9. Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap", *U.C. Davis Law Review*, Vol. 51, 2017.
10. Jack M. Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation", *UC Davis Law Review*, Vol. 51, 2018.
11. Frank Pasquale, "A Rule of Persons, Not Machines", *Michigan Law Review*, relevant scholarship concerning automated decision-making.
12. Lilian Edwards and Michael Veale, scholarship concerning explainability, automated decision-making and data protection.
13. Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies", *Harvard Journal of Law & Technology*, Vol. 29, 2016.
14. W. Nicholson Price II, "Black-Box Medicine", *Harvard Journal of Law & Technology*, Vol. 28, 2015.
15. Rebecca Crootof, "The Killer Robots Are Here: Legal and Policy Implications", relevant scholarship on autonomous systems and international law.

C. GOVERNMENT REPORTS AND POLICY DOCUMENTS

1. NITI Aayog, *National Strategy for Artificial Intelligence #AIForAll*, Government of India, 2018.
2. NITI Aayog, *Responsible AI: Approach Document for India, Part 1 – Principles for Responsible AI*, 2021.
3. NITI Aayog, *Operationalizing Principles for Responsible AI*, 2021.
4. Ministry of Electronics and Information Technology, Government of India, policy and consultation materials relating to Artificial Intelligence and emerging technologies.
5. Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act, 2023* and related policy materials.
6. Ministry of Electronics and Information Technology, *Information Technology Act, 2000* and related rules.
7. Indian Computer Emergency Response Team (CERT-In), cybersecurity advisories and directions.



8. Reserve Bank of India, reports and regulatory materials concerning Artificial Intelligence, machine learning, digital banking and financial technology.
9. Securities and Exchange Board of India, regulatory materials concerning algorithmic and technology-enabled financial services.
10. UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 2021.
11. OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, 2019.
12. European Commission, materials relating to the European Union Artificial Intelligence Act.
13. United Nations, reports and policy materials concerning Artificial Intelligence, human rights and digital governance.
14. World Economic Forum, reports concerning Artificial Intelligence, governance and emerging technologies.
15. Stanford Institute for Human-Centered Artificial Intelligence, *AI Index Report*.

D. INTERNATIONAL LEGAL AND POLICY SOURCES

1. European Union, Regulation (EU) 2024/1689 – Artificial Intelligence Act.
2. General Data Protection Regulation, Regulation (EU) 2016/679.
3. OECD AI Principles.
4. UNESCO Recommendation on the Ethics of Artificial Intelligence, 2021.
5. United Nations Guiding Principles and reports concerning AI and human rights.
6. Council of Europe materials on Artificial Intelligence and human rights.
7. United States executive and regulatory materials concerning Artificial Intelligence.
8. United Kingdom Government, *A Pro-Innovation Approach to AI Regulation* and subsequent AI governance materials.

E. ONLINE RESOURCES

The following websites may be used for academic research and verification of legal materials:

Indian Legal Resources

1. **Supreme Court of India**
<https://www.sci.gov.in/>
2. **India Code**
<https://www.indiacode.nic.in/>
3. **Ministry of Electronics and Information Technology (MeitY)**
<https://www.meity.gov.in/>
4. **NITI Aayog**
<https://www.niti.gov.in/>
5. **Indian Computer Emergency Response Team (CERT-In)**
<https://www.cert-in.org.in/>
6. **Digital Personal Data Protection / MeitY resources**
<https://www.meity.gov.in/>
7. **Delhi High Court**
<https://delhihighcourt.nic.in/>
8. **Indian Kanoon**
<https://indiankanoon.org/>

International Resources

9. **European Commission – Artificial Intelligence**
<https://digital-strategy.ec.europa.eu/>
10. **EUR-Lex – European Union Law**
<https://eur-lex.europa.eu/>



11. **OECD Artificial Intelligence**
<https://oecd.ai/>
12. **UNESCO – Artificial Intelligence Ethics**
<https://www.unesco.org/>
13. **United Nations**
<https://www.un.org/>
14. **World Intellectual Property Organization (WIPO)**
<https://www.wipo.int/>
15. **World Economic Forum**
<https://www.weforum.org/>
16. **Stanford HAI – AI Index**
<https://hai.stanford.edu/>
17. **UK Supreme Court**
<https://www.supremecourt.uk/>
18. **U.S. Courts**
<https://www.uscourts.gov/>

F. SECONDARY SOURCES

Secondary sources used for understanding and analysis include:

- textbooks on cyber law;
- books on Artificial Intelligence;
- intellectual property law commentaries;
- privacy and data protection scholarship;
- peer-reviewed law journal articles;
- government policy papers;
- regulatory reports;
- international organisation reports;
- academic research papers; and
- authoritative legal databases.

Secondary sources should be used to explain and analyse primary legal materials rather than replace statutes and judicial decisions.

IMPORTANT PRIMARY AND SECONDARY SOURCE DISTINCTION

Primary Sources

The following should be treated as primary legal authorities:

- Constitution of India;
- Acts of Parliament;
- Rules and Regulations;
- Supreme Court judgments;
- High Court judgments;
- binding judicial precedents;
- official government notifications;
- treaties and other applicable legal instruments.



Secondary Sources

The following are secondary authorities:

- books;
- journal articles;
- commentaries;
- research papers;
- reports;
- policy papers;
- legal encyclopaedias;
- academic websites.

For an LL.B. research journal, the strongest methodology is to use **primary sources for the statement of law and secondary sources for explanation, criticism and comparative analysis.**

SUGGESTED CITATION STYLE FOR THE JOURNAL

Cases may be cited as:

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

Statutes may be cited as:

Information Technology Act, 2000.

Books:

Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (Oxford University Press 2014).

Journal articles:

Sandra Wachter, Brent Mittelstadt & Luciano Floridi, “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,” 7 International Data Privacy Law 76 (2017).

Reports:

NITI Aayog, *National Strategy for Artificial Intelligence #AIForAll* (2018).

FINAL RESEARCH OBSERVATION

The principal argument of this journal is that **India does not necessarily require a technology law that merely restricts Artificial Intelligence; it requires a rights-based and risk-based framework capable of encouraging innovation while protecting privacy, dignity, equality, security, intellectual property and human autonomy.**

The future development of Indian AI law should therefore be based on five fundamental principles:

1. **Human dignity**
2. **Privacy and data protection**
3. **Transparency and explainability**
4. **Accountability and human oversight**
5. **Innovation with responsible governance**

Artificial Intelligence should remain a tool for human progress and should not become a mechanism through which legal responsibility is avoided.