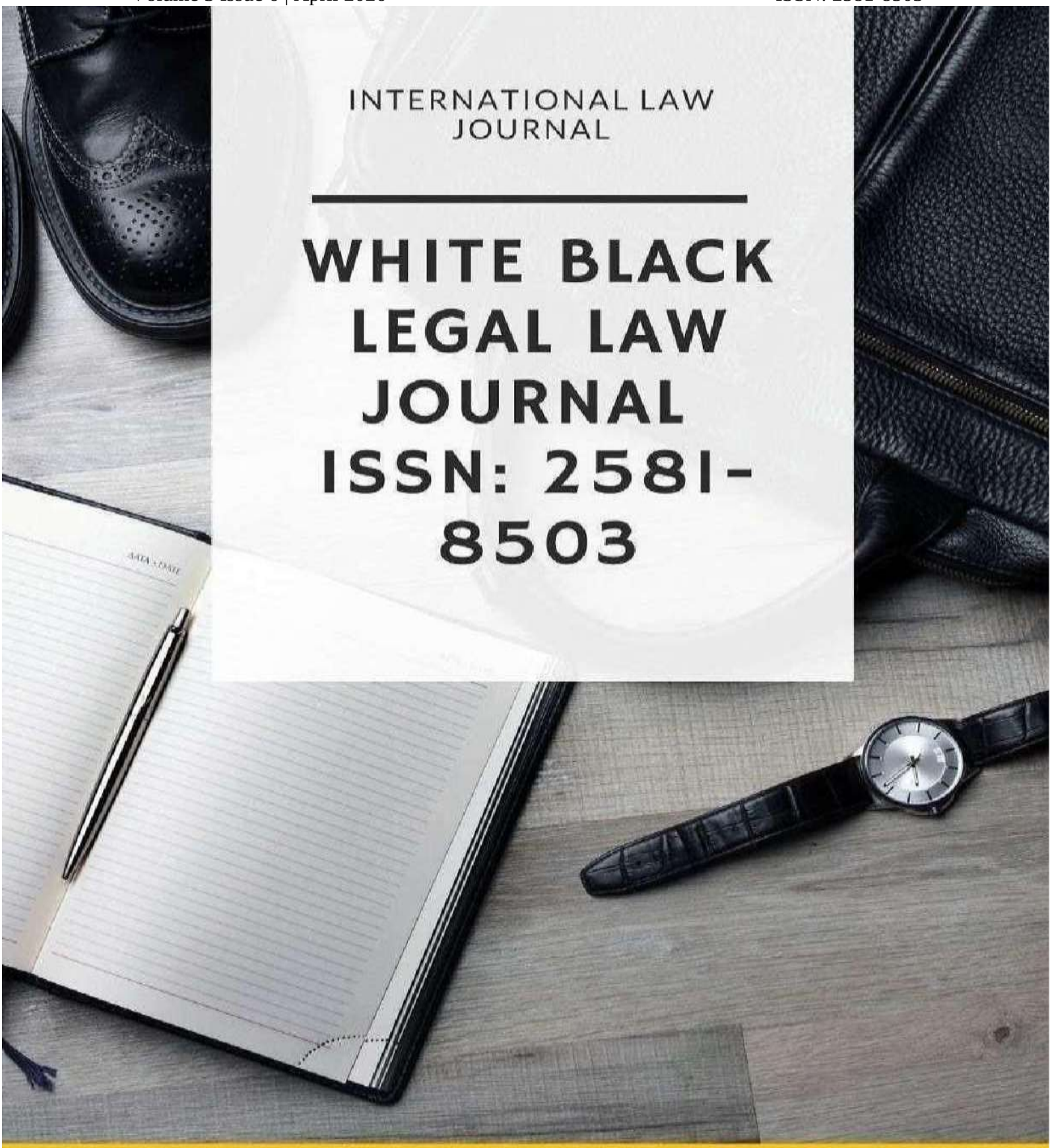

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

LEGAL CHALLENGES OF ARTIFICIAL INTELLIGENCE IN INDIA

AUTHORED BY - UTKARSHITA PATHAK
B.A. LL.B. (Hons.)
Amity Law School, Amity University

DECLARATION

I, Utkarshita Pathak, Enrollment No. A3211121107, student of B.A. LL.B. (Hons.), Amity Law School, Amity University, hereby declare that the dissertation titled "Legal Challenges of Artificial Intelligence in India" submitted in partial fulfilment of the requirements for the award of the degree of B.A. LL.B. (Hons.) is my original and independent work. This dissertation has not been submitted for the award of any other degree, diploma, or fellowship in any other university or institution.

I further declare that all information and data presented in this dissertation have been collected from authentic and verifiable sources and that all material borrowed from other sources has been duly acknowledged. Where views expressed are those of other scholars, they have been properly attributed.

I am fully aware that any misrepresentation of facts or plagiarism shall make me liable for cancellation of my degree by Amity University as per applicable rules and regulations.

Place: _____

Date: _____

Signature: _____

Utkarshita Pathak

FACULTY GUIDE APPROVAL

This is to certify that the dissertation titled "Legal Challenges of Artificial Intelligence in India" submitted by Utkarshita Pathak, Enrollment No. A3211121107, student of B.A. LL.B. (Hons.), Amity Law School, Amity University, is an original and independent piece of research work carried out under my supervision.

To the best of my knowledge, the work has not been submitted for any other degree, diploma, or fellowship in this or any other university or institution. The dissertation fulfils all requirements for submission as a NTCC Dissertation Report.

Dr. Prabhdeep Kaur Malhotra

Assistant Professor I

Amity Law School, Amity

University Date: _____

ACKNOWLEDGEMENT

First and foremost, I express my profound gratitude to my Faculty Guide, Prabhdeep Kaur Malhotra, whose scholarly guidance, intellectual rigour, and unwavering support have been the cornerstone of this research. Her patient counsel, timely suggestions, and deep knowledge of law and technology greatly enriched this work at every stage. The completion of this dissertation would not have been possible without his/her unstinting encouragement.

I am deeply grateful to the Dean and faculty members of Amity Law School for providing an intellectually stimulating academic environment that encouraged this line of inquiry. The institution's library and digital resources, including access to SCC Online, Manupatra, HeinOnline, and JSTOR, were indispensable tools in this research.

I owe a debt of gratitude to the many legal scholars, academics, and practitioners whose published works, articles, and policy documents have informed this dissertation. Their insights have deepened my understanding of the rapidly evolving relationship between law and technology in the Indian context.

I also thank my colleagues and fellow students for their companionship, constructive discussions, and moral support throughout this endeavour. Their perspectives, though informal, have sharpened my arguments and broadened my thinking.

Finally, I express my deepest appreciation to my family for their immeasurable love, constant encouragement, and unwavering faith in my abilities. Their sacrifices and support have made my academic journey possible.

Utkarshita Pathak

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AI	:	Artificial Intelligence
AIR	:	All India Reporter
Art.	:	Article
CCTV	:	Closed-Circuit Television
CPA	:	Consumer Protection Act
DPDP	:	Digital Personal Data Protection
EU	:	European Union
FRT	:	Facial Recognition Technology
GDPR	:	General Data Protection Regulation
HC	:	High Court
IPC	:	Indian Penal Code
IT Act	:	Information Technology Act
LLM	:	Large Language Model
MeitY	:	Ministry of Electronics and Information Technology
ML	:	Machine Learning
NLP	:	Natural Language Processing
NITI Aayog	:	National Institution for Transforming India
NTCC	:	Non-Teaching Credit Course
RBI	:	Reserve Bank of India
SC	:	Supreme Court
SCC	:	Supreme Court Cases
SEBI	:	Securities and Exchange Board of India
UN	:	United Nations
UNESCO	:	United Nations Educational, Scientific and Cultural Organization
WIPO	:	World Intellectual Property Organization

LIST OF CASES

Indian Cases

1. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1
3. Eastern Book Company v. D.B. Modak, (2008) 1 SCC 1
4. Indian Council for Enviro-Legal Action v. Union of India, AIR 1996 SC 1446
5. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
6. K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 (Aadhaar)
7. Kharak Singh v. State of U.P., AIR 1963 SC 1295
8. Lalit Bhasin v. Union of India, 2020 SCC OnLine SC 1109
9. M.C. Mehta v. Union of India, AIR 1987 SC 1086
10. Maneka Gandhi v. Union of India, AIR 1978 SC 597
11. Manupatra Information Solutions Pvt. Ltd. v. Google India Pvt. Ltd., CS (OS) 1340/2012 (Delhi HC)
12. Mukesh v. State for NCT of Delhi, (2017) 6 SCC 1
13. National Legal Services Authority v. Union of India, (2014) 5 SCC 438
14. Navtej Singh Johar v. Union of India, (2018) 10 SCC 1
15. People's Union for Civil Liberties v. Union of India, (2003) 4 SCC 399
16. Romesh Thappar v. State of Madras, AIR 1950 SC 124
17. Selvi v. State of Karnataka, (2010) 7 SCC 263
18. Shreya Singhal v. Union of India, (2015) 5 SCC 1

19. Shyam Sunder v. Ram Kumar, AIR 2001 SC 2472

20. State (NCT of Delhi) v. Navjot Sandhu, AIR 2005 SC 3820

21. State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808

22. Suchita Srivastava v. Chandigarh Admn., (2009) 9 SCC 1

Foreign Cases

23. Acohs Pty Ltd. v. Ucorp Pty Ltd., [2012] FCAFC 16 (Australia)

24. Blyth v. Birmingham Waterworks Co., (1856) 11 Exch. 781

25. Donoghue v. Stevenson, [1932] AC 562

26. Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991)

27. Google Spain SL and Google Inc v. Agencia Española de Protección de Datos, C-131/12, [2014] ECLI:EU:C:2014:317

28. Rylands v. Fletcher, (1868) LR 3 HL 330

29. Thaler v. Comptroller-General of Patents, Designs and Trade Marks, [2023] UKSC 49

30. Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022)

ABSTRACT

The exponential growth of artificial intelligence (AI) technologies in all sectors of our society has created a dire need for legal structures to deal with the specific challenges posed by AI systems. India, with its rapid digital transformation and ambitious AI development strategy, is particularly vulnerable to the significant regulatory gaps that AI's integration into areas as varied as health, finance, law enforcement, intellectual property and creative arts has unleashed. This dissertation engages in a thorough and critical analysis of the legal implications of AI in the Indian legal landscape, including liability and accountability, intellectual property, data protection and privacy, cybercrime and the pressing need for a regulatory framework.

The study adopts primarily a doctrinal approach, relying on primary and secondary sources of law, such as statutes, case law, judicial pronouncements of the Supreme Court and High Courts, government policy documents of the Indian Government and NITI Aayog, and scholarly literature from India and abroad. By drawing lessons from global regulatory frameworks, particularly the European Union's groundbreaking Artificial Intelligence Act 2024, the United States' Executive Order on AI, and the regulatory frameworks in China, Singapore and the United Kingdom, the dissertation highlights the significant gaps in the existing legal framework of India and proposes practical and actionable suggestions for the creation of a holistic and culturally relevant AI governance framework in India.

The dissertation concludes that while not completely bereft of relevant provisions, India's existing legal framework is structurally inadequate to cope with the complex and dynamic issues surrounding AI governance. The lack of specific AI legislation, the unresolved uncertainties in attributing liability for AI-induced harm under tort law and the Consumer Protection Act 2019, the unsettled question of authorship and inventorship of AI- generated works under the Copyright Act 1957 and Patents Act 1970, the incompleteness and weakness of the implementation of the Digital Personal Data Protection Act 2023 in relation to AI-driven data processing, and the inadequacy of existing criminal law provisions under the Indian Penal Code 1860 and the Information Technology Act 2000 to combat AI-facilitated crimes are among the prominent concerns. The dissertation offers a holistic set of principled recommendations to build a responsible, innovation-

compatible and fundamental rights-compatible AI governance framework for India that is mindful of India's socio-economic realities and development challenges.

Keywords: Artificial Intelligence, Legal Framework, India, Liability, Intellectual Property, Data Protection, Privacy, Cybercrime, AI Regulation, AI Governance, Digital Personal Data Protection

CHAPTER I

INTRODUCTION

1.1 Background and Context

The 21st century is witnessing an extraordinary technological revolution, unprecedented in scale and pace. Among the many and varied technologies underpinning this revolution, Artificial Intelligence (AI) is distinguished by its ability to mimic, and in some instances, surpass human intelligence. Since the origin of the discipline in the early theories of Alan Turing (who in 1950 asked the influential question "Can machines think?"),[1] and the initial proposals of John McCarthy and others at the Dartmouth Summer Research Project in 1955 (which coined the term "Artificial Intelligence"),[2] AI has grown from a speculative academic project to one of the most important and ubiquitous influences on human society.

Today, AI systems undertake complex tasks in an incredibly broad range of human endeavours: diagnose disease with an accuracy that matches or surpasses that of human experts, compose music and generate visual art of astonishing creativity, write legal briefs and evaluate contracts, drive cars, manage investment portfolios, sift resumes, predict criminal recidivism, and help judges determine sentences. As noted by two of the most influential AI academics, Stuart Russell and Peter Norvig, AI is the science and engineering of making intelligent machines systems that perceive their environment, learn from experience, and take actions that maximise their chances of successfully achieving their goals.[3]

India has recognised this revolutionary potential. Recognising the massive opportunity for development that AI represents, the Indian Government has put forward a bold national

[1]Alan Turing, 'Computing Machinery and Intelligence' (1950) 59 Mind 433.

[2]John McCarthy and others, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence' (Dartmouth College 1955) <http://www- formal.stanford.edu/jmc/history/dartmouth/dartmouth.html> accessed 18 April 2025.

[3]Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach (4th edn, Pearson 2020) 1.

vision in its 2018 National Strategy for Artificial Intelligence prepared by NITI Aayog, which has adopted the inclusive mantra "#AIForAll" and set its sights on transforming five sectors health care, agriculture, education, smart cities and infrastructure, and smart mobility through AI.[4] India's digital infrastructure has advanced rapidly: with more than 900 million internet users, a thriving start-up culture, world-leading software engineers and substantial governmental investment in sectors such as Digital India and the National Digital Health Mission, India is well positioned to lead the world in the development of AI.[5]

But the very features that make AI so powerful its invisibility, its potential to make decisions and act without human intervention, its capacity to learn from and draw upon vast data sets containing highly personal information, and its capacity to create works of art and make decisions with significant impact are also what raise novel and deep legal questions. The law has traditionally evolved to regulate human conduct and to define the relationships among human persons. But AI systems do not easily slot into the categories of personhood, agency and responsibility that the law has developed over the ages. If a self-driving car runs over someone and kills them, who is responsible the car manufacturer, the software developer, the car owner or the car itself? When an AI system creates a new musical composition or invention, who holds the intellectual property rights? When facial recognition software mistakenly identifies an innocent person as a criminal, what recourse is there? When algorithms are used to make important decisions about credit, employment, or bail, and the data they are trained on is biased, what law applies? These are pressing applied questions that this research will address.[6]

1.2 The Legal Landscape in India: A Preliminary Overview

India's legal framework, though robust in many areas, is not AI-specific. The primary law regulating online activities the Information Technology Act, 2000 was drafted during the pre-dynamic web period and basic e-commerce.[7] Although it has been amended in 2008 and complemented by a range of rules and regulations, it is essentially geared to traditional cybercrime and electronic governance issues, with no specific provisions for

[4]NITI Aayog, National Strategy for Artificial Intelligence: #AIForAll (Government of India 2018).
[5]Ministry of Electronics and Information Technology, India's Trillion Dollar Digital Opportunity (Government of India 2019).
[6]Ryan Calo, 'Robotics and the Lessons of Cyberlaw' (2015) 103 California Law Review 513, 521.

[7]Information Technology Act 2000 (Act 21 of 2000).

AI-generated works, autonomous systems or algorithmic governance. The Indian Penal Code, 1860, the main criminal law statute, was enacted well before the advent of the internet and does not consider crimes committed by or using AI.[8] Likewise, the Copyright Act, 1957 and the Patents Act, 1970 include provisions for the protection of intellectual property, which assume human originators and inventors, leaving AI-generated intellectual property in a state of legal limbo.[9]

The Digital Personal Data Protection Act, 2023 (DPDP Act), which was given Presidential assent in August 2023, is the most recent and important piece of digital legislation.[10] The DPDP Act establishes a framework for data privacy protection that is relevant to AI systems, which almost always rely on large data sets for training and operation. But the DPDP Act does not specifically address issues such as automated decision-making, profiling or algorithmic accountability. The Consumer Protection Act, 2019, which bolsters the product liability regime, may be relevant to defective AI products and services, but was not designed to address AI-specific concerns.[11]

The Supreme Court of India in its landmark nine-judge bench case in Justice K.S. Puttaswamy (Retd.) v. Union of India unanimously affirmed the right to privacy as a part of the fundamental right to life and liberty under Article 21 of the Constitution of India.[12] This is an important building block in the case of AI, which often involves large-scale data collection, surveillance and profiling. However, constitutional protections, in the absence of concrete legislative and institutional arrangements, cannot by themselves effectively respond to the complex and rapidly-changing issues arising from AI.

In this context of a severely deficient legal framework, the AI industry has seen rapid growth in India. The AI industry in India is growing at a rapid pace with estimates that the market size will reach USD 7.8 billion by 2025. Government agencies, courts, banks, health care, telecom, and law enforcement are all using AI systems in important decision-making settings often in a legal vacuum that poses substantial risks to individuals, businesses and society. This makes the rigorous analysis of the legal challenges of AI in India not just an academic but practical concern.

[8]Indian Penal Code 1860 (Act 45 of 1860).
[9]Copyright Act 1957 (Act 14 of 1957); Patents Act 1970 (Act 39 of 1970).
[10]Digital Personal Data Protection Act 2023 (Act 22 of 2023).
[11]Consumer Protection Act 2019 (Act 35 of 2019).

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

1.3 Statement of the Problem

The main problem addressed by this dissertation is the inability of India's legal framework to regulate the use, functioning and impacts of Artificial Intelligence. This falls short in several ways. First, it does not offer adequate mechanisms to address issues of liability where AI systems cause physical, financial, or reputational harm to society or individuals. Existing liability doctrines such as negligence, strict liability and product liability, as applicable in India, were not framed with AI systems in mind and fit, if at all, in a complicated way with the autonomous systems whose actions cannot always be attributed to one and one human actor.

Second, the existing intellectual property regime does not address fundamental questions: Is a non-human AI system an "author" or "inventor" for the purpose of Indian copyright and patent law? Is the intellectual property created by an AI system, without any significant human creative input, owned by anyone, or is it in the public domain? How will this ambiguity impact investment in AI research and development?

Third, the remarkable data processing, profiling and surveillance capabilities of AI raise serious concerns about the constitutional right to privacy in India. Although the DPDP Act 2023 offers a broad framework for data protection, it does not specifically address important AI-related aspects such as the right to explanation when relying on automated decision-making, limits on algorithmic profiling, and human oversight of important decisions made by AI.

Fourth, AI technologies enable new forms of cybercrime and other criminal harms from deepfake-based fraud and defamation, to AI-assisted phishing and social engineering, to AI-generated child sexual abuse material for which the current criminal law framework is ill-equipped to address. On the other hand, AI is being used within the criminal justice system for predictive policing, risk assessment and forensic analysis in the absence of legal protections against misuse and to ensure fairness and accuracy.

Fifth and finally, there is no holistic, coherent, risk-based governance of AI in India. In the absence of regulatory standards, guidelines, and institutions, AI development and use in India takes place in a regulatory "wild West" that leaves room for irresponsibility, misuse and harm, as well as uncertainty for responsible innovation.

1.4 Objectives of the Study

Against the backdrop of the foregoing, this dissertation pursues the following specific objectives:

(i) To examine the conceptual and technical dimensions of Artificial Intelligence and to situate the legal challenges it presents within a global comparative context, drawing lessons from the regulatory approaches of the European Union, the United States, the United Kingdom, and China;

(ii) To critically analyse the adequacy of India's existing tort law and statutory frameworks including the Consumer Protection Act 2019 to address liability and accountability for AI-caused harm;

(iii) To examine the implications of AI for intellectual property rights in India, with specific reference to the Copyright Act 1957 and the Patents Act 1970, and to assess the need for legislative amendments to address AI authorship and inventorship;

(iv) To evaluate the framework of data protection and privacy law in India including the DPDP Act 2023 and the constitutional right to privacy in the context of AI-driven data processing, algorithmic profiling, and surveillance;

(v) To examine the intersection of AI with cybercrime and the criminal justice system in India, including AI-enabled offences, the use of AI-generated evidence, and the deployment of AI in law enforcement and adjudication;

(vi) To assess the adequacy of India's existing regulatory landscape for AI and to formulate concrete, principled recommendations for the development of a comprehensive AI governance framework that balances innovation with the protection of fundamental rights and the public interest.

1.5 Research Methodology

This dissertation follows a primarily doctrinal research approach, with some comparative and policy-analytical dimensions. The doctrinal approach involves a systematic study and critical analysis of primary sources (the text of the law, regulations, constitutional provisions, judicial precedents of the Supreme Court of India and High Courts, and policy

documents of government authorities) and secondary sources (academic journal articles, books, and reports of law reform commissions and expert committees).

The comparative aspect of the research entails an analysis of the regulatory and jurisprudential frameworks of AI governance in some foreign jurisdictions, including the European Union, the United States, the United Kingdom, China and Singapore. Comparative legal analysis is undertaken not with a view to transplanting foreign legal solutions wholesale into India, but to draw lessons in the form of best practices, structural frameworks, and warning signs which can guide the design and development of an appropriate AI governance framework for India which is responsive to India's distinctive constitutional framework, development goals, and socio-economic context.

The policy-analytical component of the research includes analysis of official policies, strategies, committee reports, and regulatory guidelines of the Indian government agencies such as NITI Aayog, MeitY, RBI, SEBI, and IRDAI with relevance to AI governance. This provides insight into the regulatory landscape in India, and the key inconsistencies and gaps in the existing landscape that an AI governance framework should address.

Primary sources include the Information Technology Act 2000, the Digital Personal Data Protection Act 2023, the Consumer Protection Act 2019, the Copyright Act 1957, the Patents Act 1970, the Indian Penal Code 1860, the Indian Evidence Act 1872, the Constitution of India and the EU AI Act 2024. Secondary sources include legal databases (SCC Online, Manupatra), international databases (HeinOnline, Westlaw) and literature on AI law and governance.

1.6 Scope and Limitations

This dissertation is limited in scope, both in terms of topic and methodology. In terms of scope, the dissertation covers the civilian and criminal law aspects of AI regulation in India, particularly liability, intellectual property, data protection and privacy, cyber crime and regulatory framework. Although the dissertation refers to AI's impact in specific areas such as the health, financial and judicial sectors, it does not offer an in-depth sector-specific analysis, which would be impossible to include in a single dissertation.

In terms of methodology, the dissertation does not conduct empirical research it does not survey, interview practitioners or affected persons, or gather primary quantitative or qualitative data on the impact of AI in India. This type of empirical work, while important and necessary, would be beyond the scope of a doctrinal dissertation. The study also does not delve deeply into computer science issues with AI neural networks, training algorithms, model architecture, and so on except to the extent they give rise to legal issues.

The pace of development in the technology itself and in the legal and regulatory response to it creates a challenge for its research. Although great care has been taken to ensure that the research is up-to-date to the date of submission, this field moves at lightning pace and some specific provisions or developments may have been altered.

1.7 Significance of the Research

The research contributes in multiple ways to the nascent field of AI law in India. First, it offers the first systematic analysis of the legal challenges of AI in all the relevant fields of law liability, intellectual property, data protection, criminal law and regulation in a single scholarly contribution. Although specific dimensions of AI law in India have been discussed in journal articles and policy briefs, previous research has not attempted to bring together these multiple dimensions.

Second, it offers a contemporary analysis of India's most recent legal development in the digital space the Digital Personal Data Protection Act 2023 as part of an analysis of AI governance more broadly that is currently absent in the literature. Third, the research's comparative analysis, which draws on the EU AI Act 2024 and other international frameworks, offers Indian policymakers and legislators a nuanced understanding of the best practices in the global arena and how they might be adapted to the Indian context.

Fourth and most importantly, the research offers a normative contribution by providing evidence-based recommendations for the creation of an AI governance framework for India. These recommendations are based on India's constitutional values (particularly the fundamental rights to equality, life and personal liberty and freedom of speech) as well as on best practices and India's developmental priorities. In a policy context where AI governance has become a priority on the legislative agenda, such evidence-based recommendations are useful.

1.8 Chapter Scheme

The dissertation has eight chapters. Chapter I, the present chapter, provides the introduction, setting out the background and context, statement of the problem, objectives, methodology, scope and limitations, significance, and structure of the research.

Chapter II provides an overview of the conceptual and technical underpinning of Artificial Intelligence, bringing into the conversation about law and AI an understanding of the scope and limitations of AI. It chronicles the historical development and evolution of AI, reviews the major types of AI systems (from narrow to general AI) and the use of AI in India. It then undertakes a comparative overview of the regulatory landscape globally, and focuses on the EU AI Act 2024, the United States and regulatory developments in other jurisdictions.

Chapter III focuses on the key issues of civil liability and accountability for harms caused by AI in India. It discusses the application of general tort law principles negligence, strict liability, and absolute liability to AI-caused harm, the product liability regime under the Consumer Protection Act 2019, and the issues of liability in the specific contexts of autonomous vehicles, medical AI, and AI in financial services.

Chapter IV examines the impact of AI on intellectual property in India. It explores questions of authorship and ownership of AI-driven creative works under the Copyright Act 1957, questions of AI inventorship under the Patents Act 1970, and other related issues of trade secrets and data rights in the context of AI.

Chapter V discusses the issues of AI and data protection and privacy rights in India. It examines the right to privacy as enunciated in the Puttaswamy case, the sufficiency of the DPDP Act 2023 to regulate AI, and concerns around profiling, facial recognition and surveillance in the context of AI.

Chapter VI explores AI and cybercrime and criminal justice. It considers AI-driven cybercrimes such as deepfakes, AI-assisted disinformation, and algorithmic scams, assesses the sufficiency of the IPC and IT Act in dealing with these crimes, and explores the role of AI in policing, predictive policing, and judicial decision-making.

Chapter VII draws on the insights from the earlier chapters to critically evaluate the current state of India's AI governance and to provide a set of recommendations on AI governance. Drawing insights from global developments and India's constitutional and developmental priorities, it offers specific policy, institutional and legal recommendations.

The dissertation concludes in Chapter VIII with an overview of the key findings and contributions, and an outlook for future work.

1.9 India's Constitutional Framework and AI Governance: A Preliminary Assessment

India's constitutional framework provides the normative foundation upon which any AI governance regime must be constructed. The Constitution of India, a living and transformative document, enshrines in Part III a set of fundamental rights that have direct and significant bearing on the regulation of AI systems. The constitutional guarantees of equality before the law and equal protection of laws under Article 14, the prohibition of discrimination on grounds of religion, race, caste, sex or place of birth under Article 15, and the right to life and personal liberty under Article 21 collectively constitute the constitutional bedrock of AI governance in India.[13]

The transformative power of judicial interpretation has progressively expanded these fundamental rights in ways directly relevant to AI regulation. In a series of landmark constitutional decisions, the Supreme Court of India has interpreted Article 21 to embrace a wide cluster of rights, including the right to privacy, the right to dignity, the right to livelihood, the right to health and access to justice, and the right to education.[14] All of these rights are potentially affected by algorithmic systems: an AI system that denies a person a loan, removes them from a beneficiary list, predicts their likelihood of committing a crime, or misidentifies them as a security threat may directly implicate the constitutional right to life, liberty, dignity and livelihood. The question for AI governance is whether the constitutional framework, as currently interpreted, is sufficient to check these harms or whether specific legislative and institutional mechanisms are needed.

[13]Navtej Singh Johar v Union of India (2018) 10 SCC 1.
[14]National Legal Services Authority v Union of India (2014) 5 SCC 438.

The directive principles of state policy in Part IV of the Constitution, while not directly enforceable in courts, provide important normative guidance for AI governance. Article 38, which directs the state to secure a social order for the promotion of the welfare of the people, Article 39A which provides for equal justice and free legal aid, and Article 41 which provides for the right to work and public assistance in certain cases, are all relevant to the deployment of AI in a manner that distributes its benefits equitably and does not exacerbate existing inequalities. The Supreme Court has repeatedly held that fundamental rights and directive principles must be read harmoniously, and a responsible AI governance framework must reflect both dimensions of India's constitutional project.[15]

The fundamental right to freedom of speech and expression under Article 19(1)(a) has significant implications for AI-generated content, including deepfakes, AI-generated disinformation, and AI-driven content moderation on digital platforms.[16] The proportionality standard that the Court applies to restrictions on free speech under Article 19(2) must be applied with equal rigour to legislative and administrative measures that seek to restrict or require disclosure of AI-generated content. Any regulatory regime that imposes blanket restrictions on AI-generated speech without adequate procedural safeguards runs the risk of being struck down as unconstitutional.

India's constitutional scheme also presents questions of federalism and separation of powers with implications for AI governance. AI regulation touches upon a wide range of subjects that straddle the Union, State and Concurrent Lists under the Seventh Schedule from public order and policing (State List) to communications and broadcasting, banking, and inter-state trade and commerce (Union List) to criminal law and civil procedure (Concurrent List). A comprehensive horizontal AI Governance Act enacted by Parliament would need to be carefully drafted, relying primarily on the Union's powers under Entry 97 of the Union List (residuary powers) or Entry 31 (posts, telegraphs, telephones) to ensure its constitutional validity across the full range of AI applications.[17]

India's engagement with international human rights obligations, reflected in Article 51 of the Constitution, also provides a normative context for AI governance. India has ratified the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), whose provisions are

[15]People's Union for Civil Liberties v Union of India (2003) 4 SCC 399.
[16]Shreya Singhal v Union of India (2015) 5 SCC 1.

[17]Lalit Bhasin v Union of India 2020 SCC OnLine SC 1109.

directly relevant to the right to privacy, right to equality, and right to a fair trial in the context of AI decision-making. The Supreme Court has held that international conventions to which India is a party can be used to interpret domestic fundamental rights provisions, which makes the international human rights framework relevant to judicial review of AI-related state action.

CHAPTER II

ARTIFICIAL INTELLIGENCE: CONCEPTUAL FRAMEWORK AND THE GLOBAL REGULATORY LANDSCAPE

2.1 Introduction

In order to undertake an examination of the legal implications of Artificial Intelligence, it is first necessary to provide an overview of the nature of the technology and its many uses. Legal analysis of a technology requires a certain degree of familiarity with the technology, its functions, capabilities, and limitations, as well as its differences from previous technologies. This chapter therefore sets out a definition of AI, outlines the various types of AI systems and the applications of these systems, traces the history of AI development, and includes a comparative study of the global regulatory environment.

2.2 Defining Artificial Intelligence

There is no accepted definition of Artificial Intelligence. Coined by John McCarthy in 1956, the term has been defined in discrete ways by researchers, organisations and regulators for various purposes. In this dissertation, AI is defined as computer systems that perform tasks that are normally thought to require human intelligence such as learning, reasoning, problem-solving, perception, natural language processing and decision-making. This broad definition includes a diverse range of technologies, from rule-based expert systems to more complex machine learning models that are capable of adaptive learning.

A key differentiation in the AI field is between Artificial Narrow Intelligence (ANI) and Artificial General Intelligence (AGI). ANI (or weak AI) is the term used to describe AI systems that are trained to perform a narrow task such as image recognition, language translation or game-playing. This is the form of AI that is available today. AGI, on the other hand, is a hypothetical type of AI with the general intelligence of a human being,

that can perform any cognitive task that a human can.[18] There is no AGI currently in existence, but it is an aim of some research.

It is helpful to examine the definition of AI used by the European Union in its Artificial Intelligence Act of 2024, which is the most sophisticated world instrument for regulating AI. An AI system is defined in the EU AI Act as a machine-based system that, for a given set of objective functions to optimise, is designed to operate with varying levels of autonomy and that, based on the data it receives, can infer how to best achieve those objective functions by producing outputs such as predictions, recommendations or decisions that can be used to influence its physical or virtual environments.[19] This definition is admittedly complex, but illustrates the key characteristics that are legally relevant to AI: autonomy, adaptiveness and the ability to affect the physical or virtual environment through its outputs.

2.2.1 Machine Learning and Deep Learning

The most common type of AI today is machine learning (ML), in which systems learn and make decisions from data, rather than being programmed by humans.[20] Computer programming typically involves human programmers hard-coding rules into computer programs; in contrast, ML systems learn to follow rules from data. This paradigm shift has two significant legal implications: first, the behaviour of ML systems cannot be fully understood or predicted, even by their designers, because the "rules" that they follow are encoded in millions or billions of numerical parameters that are learned from data; second, ML systems can learn, reinforce, or even create biases from their training data, which can have discriminatory and adverse effects on individuals and groups.

Deep learning, a type of machine learning that uses artificial neural networks with many layers, has underpinned many of the major recent breakthroughs in AI, such as the large language models (LLMs) like GPT-4 and Claude that generate natural, coherent, and contextually relevant text; image classification systems that predict disease from medical images; and generative artificial intelligence (AI) systems that create and generate synthetic images, videos, and audio. These capabilities raise a range of novel legal

[18]Nick Bostrom, Superintelligence: Paths, Dangers, Strategies (Oxford University Press 2014) 22.

[19]Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (AI Act) [2024] OJ L, art 3(1).

[20]Tom M Mitchell, Machine Learning (McGraw-Hill 1997) 2.

questions such as authorship of AI-generated works, use of AI to generate malicious synthetic videos (deepfakes) and suitability of the law to govern AI systems whose operations are essentially a black box.[21]

2.2.2 AI Applications in India

In India, AI is being applied in many different areas, with potentially far-reaching social impacts in both positive and negative ways enabling major social benefits on one hand, and creating new legal challenges on the other. In medicine, AI is being used to detect diabetic retinopathy, tuberculosis and cancers from medical images, with a number of initiatives backed by the National Health Authority and the National Institution for Transforming India (NITI Aayog).[22] In farming, AI-based models are being used for crop disease monitoring, weather forecasts and market price forecasts in mobile apps for millions of small farmers.

In finance, AI is widely used for credit risk assessment, fraud monitoring, algorithmic trading and chatbots. The Reserve Bank of India (RBI) has recognised that AI has a great deal of promise for financial services, but also presents risks, such as the dangers of algorithmic bias in credit scoring and the risks of correlated algorithmic trading.[23] In policing, AI-based facial recognition systems are being used by some state police forces, with attendant concerns about privacy, accuracy and a risk of algorithmic bias against marginalised groups.

In the judiciary, the Supreme Court of India's SUPACE (Supreme Court Portal for Assistance in Courts' Efficiency) initiative deploys AI to support the court's research and case management, an example that both illustrates the promise of AI in improving the efficiency of the judiciary and the risks AI poses to the independence, fairness, and humanity of the administration of justice. The use of AI in critical public decision-making scenarios (such as courts, law enforcement, and public benefits) makes the creation of legal protections all the more necessary.

2.3 Global Regulatory Landscape: A Comparative Survey

[21]Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015) 6.
[22]National Health Authority, Digital Health Blueprint (Government of India 2019).
[23]Reserve Bank of India, Report of the Working Group on Digital Lending including Lending through

Online Platforms and Mobile Apps (RBI 2021).

In recent years, there has been an explosion of national and regional regulatory efforts to regulate AI. This variety of regulatory responses is a function of both the newness of the challenges posed by AI, and the different priorities, values and governance cultures of different jurisdictions. This international regulatory environment provides an important context for understanding the regulatory challenges and opportunities facing India.

2.3.1 The European Union: The AI Act 2024

The European Union's Artificial Intelligence Act, which came into effect in August 2024, is the first global, binding regulatory model to be established specifically to regulate AI.[24] The EU AI Act adopts a risk-based approach to regulate AI, with four levels of risk: unacceptable risk (banned), high risk (subject to strict rules), limited risk (subject to transparency rules) and minimal risk (not regulated).

AI systems presenting unacceptable risk are banned outright by the EU AI Act. These include AI systems that manipulate or deceive humans through subliminal techniques resulting in behaviour that causes harm; AI systems exploiting the vulnerabilities of a particular group of individuals; AI systems for social scoring by public authorities; and, with some exceptions, real-time remote biometric identification systems for law enforcement purposes in public spaces. AI systems that pose high risk those used in critical infrastructure, education, employment, essential services, law enforcement, migration and administration of justice are subject to a long list of obligations relating to data governance, technical documentation, transparency, human oversight, accuracy, robustness and cybersecurity.

The EU AI Act also requires providers of AI systems to register high-risk systems in a public EU-wide database, and imposes significant penalties for non-compliance: fines of up to €35 million or 7% of annual global turnover for violations of prohibited AI practices, and up to €15 million or 3% of annual turnover for other violations.[25] The EU AI Act is a global precedent for AI regulation, and is already playing a key role in shaping debates around regulatory frameworks elsewhere, such as in India.

2.3.2 United States

[24]Regulation (EU) 2024/1689 (n 15).

[25]ibid, art 99.

The US has so far adopted a more sectoral and voluntary approach to regulating AI, instead of a horizontal framework for AI. The US Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, released in October 2023, required federal agencies to develop AI guidelines and standards for their sectors, mandated that developers of high-impact AI systems must report to the government the results of safety testing their systems, and directed the establishment of standards for watermarking and labelling AI content.[26] The US National Institute of Standards and Technology (NIST) has published an AI Risk Management Framework offering voluntary guidance on the responsible development and use of AI.

At the state level, some US states have passed legislation on AI, such as transparency requirements for AI-based hiring processes, limitations on police use of facial recognition technology, and disclosure requirements for AI-based political ads. The US approach, which is less restrictive of innovation than the EU model, has been criticised for leaving gaps in regulation, especially in relation to civil rights and privacy.

2.3.3 China

China has taken a proactive, application-specific approach to the regulation of AI, with the release of a raft of specific regulations for various AI technologies. The Provisions on the Management of Deep Synthesis Internet Information Services (2022) govern deepfakes and other forms of AI-generated content, mandating watermarking and consent. In contrast, the Interim Measures for the Management of Generative Artificial Intelligence Services (2023) regulate services that use large language models, requiring service providers to moderate content, ensure data security, and be transparent about their algorithms.[27] These rules reflect China's priorities for innovation and government control of information.

2.3.4 United Kingdom

The UK, since its exit from the European Union, has opted for a pro-innovation, principles-based framework to govern AI. Instead of a dedicated AI law, the UK

[26]Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed Reg 75191 (30 October 2023) <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence> accessed 18 April 2025.

[27]Cyberspace Administration of China, Interim Measures for the Management of Generative Artificial Intelligence Services (2023) <https://www.cac.gov.cn> accessed 18 April 2025.

Government has instructed existing sector regulators to implement cross-cutting principles of AI safety, transparency, fairness, accountability and contestability within their respective jurisdictions, in line with guidance from the AI Safety Institute, the world's first government institution dedicated to the safety of advanced AI models, established in November 2023.[28] The UK's approach is a welcome contrast to the EU's more rigid approach, although it has been criticised for the potential for under-regulation of AI risks.

2.3.5 India's Regulatory Position

India's regulatory approach to AI has been largely aspirational to date. The Government's National Strategy for Artificial Intelligence (2018) and the follow-up Responsible AI for All reports by NITI Aayog (2021) have set out principles for responsible AI such as inclusiveness, non-bias, safety, transparency, accountability, privacy and security, and respect for rule of law but these are not enforceable by law.[29] The MeitY's Expert Committee on AI (2023) has outlined principles for AI governance but as of the time of this study, India has not passed any AI-specific laws.[30]

This absence of AI-specific legislation in India is not entirely without justification: there are legitimate arguments that premature or poorly designed AI regulation could stifle India's nascent AI industry and its potential to serve as a global AI hub. However, the ongoing governance vacuum creates serious risks of AI-enabled harm, of discriminatory AI applications, of privacy violations, of AI-generated disinformation that India cannot afford to ignore. The chapters that follow analyse these risks in detail and make the case for specific legislative and regulatory interventions.

2.4 AI Ethics and International Standards

The rapid development of AI has prompted a significant global discussion on the ethical principles that should govern the design, development, and deployment of AI systems. This discussion has produced a rich body of ethical frameworks and guidelines,

[28]UK Government, A Pro-Innovation Approach to AI Regulation (Department for Science, Innovation and Technology 2023) <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach> accessed 18 April 2025.
[29]NITI Aayog, Responsible AI for All: Adoption Strategy for AI by the Government (Government of India 2021).
[30]Ministry of Electronics and Information Technology, Report of the Expert Committee on AI Governance (Government of India 2023) <https://www.meity.gov.in> accessed 18 April 2025.

emanating from governments, intergovernmental organisations, civil society, and the AI industry, that together constitute an international soft law framework for AI ethics. While these frameworks are generally non-binding, they have been highly influential in shaping the regulatory frameworks discussed above and provide important normative resources for the development of a values-based AI governance framework in India.

The most globally significant of these is the UNESCO Recommendation on the Ethics of Artificial Intelligence, adopted by the UNESCO General Conference in November 2021, which is the first global normative instrument on AI ethics.[31] The UNESCO Recommendation establishes a comprehensive set of values and principles for AI, including respect for human rights and dignity, fairness and non-discrimination, sustainability, privacy and data protection, transparency and explainability, responsibility and accountability, and safety and security. It also provides specific policy recommendations on data governance, the environment, gender, education, research, culture, and the economy. India, as a UNESCO member state, has endorsed the UNESCO Recommendation, which provides an important international normative foundation for India's AI governance framework.

The OECD Principles on Artificial Intelligence, adopted in May 2019 by the OECD Council and subsequently endorsed by G20 leaders, represent another important international soft law framework for AI governance.[32] The OECD Principles provide that AI should be: inclusive growth, sustainable development and well-being oriented; human-centred and respectful of values and fairness; transparent and explainable; robust, secure and safe; and accountable. These principles have been influential in shaping national AI strategies and regulatory frameworks, including India's NITI Aayog reports on responsible AI.

The G20, chaired by India in 2023, adopted the New Delhi Declaration that endorsed the OECD Principles on AI and called for international cooperation on AI governance, including on technical standards, risk frameworks, and the AI-related aspects of global digital infrastructure.[33] India's G20 Presidency played an important role in advancing the

[31]UNESCO, Recommendation on the Ethics of Artificial Intelligence (UNESCO 2021).
[32]Organisation for Economic Co-operation and Development, OECD Principles on Artificial Intelligence (OECD 2019).

[33]Group of Twenty, G20 New Delhi Leaders' Declaration (G20 2023) Annex on AI Governance.

global conversation on AI governance, and India's AI governance framework can draw legitimately on the international consensus that emerged through these processes.

The AI governance debate has also highlighted several inherent tensions that Indian policymakers must navigate. The tension between AI safety and innovation is one dimension, but equally important is the tension between stringent AI regulation and the right to development. Several developing countries have expressed concern that AI regulation designed primarily in developed-country contexts may inadvertently impede the ability of developing countries to leverage AI for development purposes.[34] India, occupying a unique position as both a developing country with major developmental challenges and a significant AI power with global technological ambitions, must navigate these tensions thoughtfully in designing its AI governance framework.

Ethical frameworks for AI have also been produced by industry actors, including major technology companies, as well as by civil society organisations.[35] While these private ethical frameworks are not enforceable, they have influenced the practice of AI development and the public debate on AI governance. The AI ethics principles developed by Indian companies and research institutions including the Tata Institute of Fundamental Research, the Indian Institutes of Technology, and others provide important domestic inputs into the development of an Indian AI governance framework that is culturally grounded and responsive to Indian conditions.

A critical observation that emerges from this comparative survey is that effective AI governance requires more than a set of aspirational principles: it requires a legal framework with binding norms, institutional infrastructure with enforcement powers, technical standards with clear metrics, and participatory processes that incorporate the voices of affected communities. India has the normative resources in its constitutional values, its international commitments, and the principles articulated by NITI Aayog and MeitY to construct such a framework. What is needed now is the political will and legislative action to translate these resources into effective governance.

[34]Luciano Floridi and others, 'An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28 Minds and Machines 689.

[35]Jack Balkin, 'The Three Laws of Robotics in the Age of Big Data' (2017) 78 Ohio State Law Journal

1217, 1221.

CHAPTER III

LIABILITY AND ACCOUNTABILITY FOR AI-INDUCED HARM UNDER INDIAN LAW

3.1 Introduction

One of the most urgent and practically significant legal issues of the age of Artificial Intelligence is the question of who is legally responsible in those cases when an AI system causes harm. The role of liability rules is much broader than a remedial role in terms of compensating people harmed by AI systems: liability rules also play an essential role in deterrence, making developers, manufacturers, and users of AI systems have an incentive to invest in safety and to take care in designing, testing, and implementing their systems. The sufficiency of the legal system of liability to AI-induced damage is thus a key aspect of any evaluation of its AI governance framework.

In this chapter, the author discusses the liability position based on the Indian law of AI-caused harm. It discusses how traditional tort law principles of negligence, strict liability and absolute liability would apply to AI-related cases; how the Consumer Protection Act 2019 would apply in the liability of products and services in the AI context; the particular and complicated liability issues presented by autonomous vehicles, AI in healthcare, and AI in financial services; and whether AI-enabled harm could be the subject of criminal liability. The chapter outlines the major gaps and ambiguities of the current liability framework in India and puts forward policy-specific suggestions of reforms.

3.2 The Challenge of Attributing Liability to AI Systems

The inherent issue of AI liability lies in the fact that AI systems are not regular products or regular services they are unique in their specifics. The conventional product liability law presupposes a comparatively straightforward sequence of causality: a manufacturer creates a product with a defect, this defect leads to injury of a consumer or a third party, and the manufacturer is to be held responsible. The malfunction be it in the design, the

manufacturing fault or the failure to warn can usually be traced back to a particular decision or procedure that was under the control of the manufacturer.

The situation with AI systems, however, is completely different. The behaviour of an AI system is not fixed according to the designers or manufacturers; rather, it is a result of the interplay between the architecture of the system and the huge datasets that the system is trained on, and the particular inputs to which the system is exposed during deployment. An AI system can be safely tested but harmful when deployed when it experiences an edge case or a distributional shift a scenario that is not covered by the distribution of its training data. Further, the problem of opaqueness of complex machine learning algorithms, whose inner decision-making mechanisms are not easily comprehensible even by their designers, compounds the effort to determine why a particular AI decision was arrived at, not to mention the possibility of apportioning blame of harmful decisions to a particular actor.[36]

Such characteristics of AI systems give rise to what researchers have described as the "responsibility gap" the likelihood that an AI system will cause harm that cannot be attributed to any particular human actor who is held fully morally and legally liable, as the harm was not intentional, not predictable from the viewpoint of any particular actor, and not a result of any clear omission of a reasonable standard of care. The challenge of normative responsibility in AI liability law is how to address this responsibility gap without diminishing the incentive to innovate AI.

3.3 Negligence and the Standard of Care

In most common law jurisdictions, negligence is the tort upon which the Indian law is based. According to the traditional definition of negligence, the plaintiff must prove: (i) that the defendant owed the plaintiff a duty of care; (ii) that the defendant breached the duty by failing to meet the standard of care as required in the situation; (iii) that the breach caused injury to the plaintiff; and (iv) that the harm is of a kind that is

[36]Robert Sparrow, 'Killer Robots' (2007) 24 Journal of Applied Philosophy 62, 69.

foreseeable.[3738] The prime Indian Supreme Court negligence cases create the identical fundamental framework.[39]

The implementation of the negligence framework to AI-related harm brings about significant challenges at every one of its four aspects. The analysis of the duty of care means that courts need to identify who out of the potentially vast number of actors in the development and deployment of an AI system (the developer of the AI model, the data provider, the system integrator, the platform operator, the end-user) owed a duty of care to the injured party. Although it would be quite plausible that courts would state that, in most cases of AI liability, there exists a duty of care, the scope and content of this duty in the AI context remain terra incognita in Indian law.

The question of standard of care is also problematic in the AI setting. What constitutes the use of reasonable care in the creation of an AI system? Does it need to be tested to exhaustion under every conceivable circumstance? Is it necessary that explainable AI methods are used? Is it necessary to continuously monitor the system performance after deployment? The responses to these questions will be very context-specific, depending on the possible damage of the AI system, the possibility to take precautions, and the level of knowledge in the technical field in question. Indian courts that lack expert technical knowledge will have a tough time determining whether specific AI developers or deployers adhered to the relevant standard of care.

The most acute challenge is the requirement of causation. Where an opaque AI system takes a decision resulting in harm, it may prove practically impossible to prove that the defendant was negligent and not some other factor without information about the internal decision logic of the AI system. This is the black box problem, in its legal form: what makes modern machine learning systems so effective makes their legal responsibility a problem. The problem has not yet been directly faced in Indian courts, and there is a paucity of guidance offered by the current jurisprudence of negligence.

3.4 Strict and Absolute Liability

[37]Blyth v Birmingham Waterworks Co (1856) 11 Ex 781.
[38]Donoghue v Stevenson [1932] AC 562.

[39]Shyam Sunder v Ram Kumar AIR 2001 SC 2472.

The drawbacks about the negligence framework have prompted academics to propose that strict liability or absolute liability principles can offer more suitable foundations of AI liability in some cases. The English case of Rylands v. Fletcher established the principle of strict liability without evidence of negligence according to this case, an individual who introduces into his land a thing that he can reasonably foresee to cause mischief should it escape shall remain liable therefore.[40] A form of strict liability has been used in the Indian Supreme Court when it comes to cases of inherently dangerous activities.[41]

More importantly, the Indian Supreme Court expressed the doctrine of absolute liability in the historic M.C. Mehta v. Union of India case, which extended far beyond the historic doctrine of strict liability by eliminating the exceptions that have historically been present under Rylands v. Fletcher.[42] The Court determined that a business that operates a hazardous or otherwise dangerous operation that results in damage to the environment or to any workers and people living in the vicinity has an absolute duty that cannot be avoided by referring to any exceptions to compensate everyone who is impacted by the accident. The business can also be forced to pay damages in terms of compensation relating to its wealth.

The absolute liability principle evolved in M.C. Mehta v. Union of India would have significant potential applicability to AI liability, especially in high-risk AI systems used in situations where the damage is predictable and potentially disastrous. It can be argued with considerable force that the use of AI systems in safety-related scenarios autonomous vehicle operation, AI-assisted surgery, and AI-controlled infrastructure management invokes, within the meaning of the M.C. Mehta doctrine, absolute liability when it comes to any harm involved. Nevertheless, the applicability of the doctrine to AI has not been firmly established by Indian courts, and it is uncertain how the doctrine would be practically applied to the multi-party AI supply chain.

3.5 Product Liability under the Consumer Protection Act 2019

The Consumer Protection Act 2019, which has majorly enhanced the system of product liability in the Indian market, is directly applicable to AI-induced damages in

[40]Rylands v Fletcher (1868) LR 3 HL 330.
[41]Indian Council for Enviro-Legal Action v Union of India AIR 1996 SC 1446.
[42]M.C. Mehta v Union of India AIR 1987 SC 1086.

commerce.[43] The CPA 2019 Chapter VI provides a specific product liability regime, according to which a product manufacturer, a product service provider, or a product seller can be found liable to compensate a consumer who suffered harm as a result of a faulty product, or a service deficiency. The Act imposes product liability on three bases: (i) manufacturing defect; (ii) design defect; and (iii) failure to warn consumers about risks of the product.

AI systems or products that contain AI elements can theoretically be subjected to product liability under the CPA 2019. A medical diagnostic device based on AI that results in a false diagnosis thereby causing the patient harm may possibly constitute a defective product within the definition of the Act. A self-driving vehicle that crashes because of a faulty navigation algorithm could be the subject of a product liability lawsuit (design defect). Nonetheless, the implementation of the particular provisions of the Act to AI products is fraught with several challenges.[44]

The definition of "defect" in the Act where the product fails to meet the relevant standards or reasonable expectations is hard to extend to AI systems whose behaviour is necessarily probabilistic and statistical, such that an AI medical diagnostic system with a 95% accuracy is not defective merely because it is wrong 5% of the time, and the patient who is within that 5% of incorrect diagnosis may in fact face very real harm.

The failure to warn ground of product liability can be especially applicable in the context of AI, as AI developers and deployers regularly do not give users and victims of their AI systems any meaningful information regarding the limitations, failure modes, and risks of their AI systems. The disclosure requirements and informed consent provisions of the CPA 2019 might be the foundation of product liability claims in cases where AI providers do not disclose issues or limitations of their systems that they are aware of.

3.6 Vicarious Liability and AI

The doctrine of vicarious liability where a tort is committed by another individual, often in the context of an employment or agency relationship is another possible basis of AI liability. The application of AI in business settings can frequently be discussed in the

[43]Consumer Protection Act 2019 (Act 35 of 2019), s 84.
[44]Andrei Popescu, 'The Liability of Autonomous AI: A Comparative Analysis' (2022) 18 Journal of

Comparative Law 112, 119.

framework of principal-agent relations: the principal (i.e. the organisation implementing an AI system to make decisions on its behalf) is responsible for the actions of the system, similarly to the case of the employer being vicariously liable for the torts the employee commits during employment.

But as AI systems gain increased autonomy, and the capacity to make independent decisions, the analogy to employment is further stretched. The vicarious liability doctrine has long held that the employee or agent must be acting under the control and direction of the principal; however, a sufficiently autonomous AI system can make decisions that its developer or deployer might not be able to predict or control, and characterising its actions as "acting on behalf of" any particular human principal may be hard. This leads to the conclusion that a specific legislative framework needs to be developed that clearly deals with the liability of AI operators for harms inflicted by the systems that they deploy.

3.7 Liability for Autonomous Vehicles

The liability issues posed by autonomous vehicles (AVs) help highlight the issue of AI liability more broadly, as AVs are one of the most commercially developed and socially significant AI applications that are being rolled out or tested now, and due to the fact that they have a direct and obvious potential to cause physical harm. India is yet to enact specific laws to regulate autonomous vehicles and the Motor Vehicles Act 1988 the main law of road transport was not made to consider autonomous vehicles.[45]

The current Indian law on liability for accidents caused by AVs is very unclear. The Motor Vehicles Act offers strict liability for an owner of a vehicle for accidents caused by its use, with compensation through the Motor Accidents Claims Tribunal system. However, applying this framework to a scenario in which an AV leads to an accident begs some tough questions: Does the owner of the vehicle bear the primary responsibility, even when the accident was due not to the negligence of the owner, but to a software fault? Does the CPA 2019 impose liability on the AV manufacturer on account of design flaw? Can the developer of the AI software be held responsible? AV liability is one of the most challenging and pressing AI liability issues that Indian law has to deal with due to the multiplicity of possible defendants and the challenge of proving causation and fault.

[45]Motor Vehicles Act 1988 (Act 59 of 1988).

3.8 Liability for AI in Healthcare

There are acute liability issues associated with the implementation of AI in healthcare settings. The application of AI systems is gaining momentum in India to support diagnostic decisions based on medical images, patterns of disease, prescription of treatment schemes and, in some cases, autonomous medical interventions. In cases where an AI system gives a wrong diagnosis or suggests unsuitable treatment which causes the patient harm, the liability issue becomes multifaceted.

Healthcare services, under the Consumer Protection Act 2019, form part of the definition of services to which a "deficiency in service" can attract liability.[46] The Act has led to the liability of doctors and hospitals in medical negligence cases. The question is how this framework fits into a situation where an AI diagnostic tool operated by a physician causes harm: is the physician negligent in accepting the false recommendation of the AI? Does the hospital bear a duty in implementing a faulty AI system? Is the AI programmer responsible for the malfunction of the system? These issues are yet to be clarified in Indian law, and the lack of clarity in this area leaves both patients needing redress and healthcare providers and AI companies debating their respective obligations.

The practice in other countries indicates that the standard of care to be applied to AI-assisted medical practice might change to require physicians to exercise independent clinical judgment despite the use of AI decision support tools meaning that a physician who simply follows an AI recommendation without his or her own assessment could be found negligent. This however places doctors in a challenging position when AI tools have been shown to appear more accurate than human judgment in particular diagnostic situations, as has already been demonstrated in the detection of some cancers and eye conditions. A more structured solution would provide a set of guidelines on how AI can be used in medical practice, the responsibilities of AI providers, and how the liability should be divided among the various parties in the AI healthcare value chain.

3.9 Liability for AI in Financial Services

The financial services sector presents a distinctive set of AI liability issues arising from the pervasive use of algorithmic systems in credit scoring, investment management,

[46]Indian Medical Association v V.P. Shanta (1996) 6 SCC 651.

insurance pricing, and fraud detection. These systems make consequential decisions about individuals' access to financial resources decisions that can have a profound impact on livelihoods, opportunities, and economic security. The liability framework applicable to AI-enabled financial harm in India is governed primarily by the Consumer Protection Act 2019, sector-specific regulations issued by the Reserve Bank of India and the Securities and Exchange Board of India, and the general law of contract and tort.[47]

The Reserve Bank of India has issued guidelines on digital lending that impose obligations on regulated entities, including those using AI-based credit scoring systems, to ensure transparency, fairness, and grievance redress.[48] The RBI's framework requires lenders to disclose the basis of credit decisions to borrowers and to provide an effective grievance redress mechanism. However, these guidelines do not specifically address the accountability of algorithmic systems in credit scoring, and do not require lenders to disclose the features or weights used by an AI model in making a credit decision a significant limitation given that the opacity of such systems makes it impossible for borrowers to understand or challenge the basis of adverse decisions.

The Securities and Exchange Board of India (SEBI) has issued a circular on the use of artificial intelligence and machine learning by market intermediaries, which requires such intermediaries to maintain detailed logs and audit trails of AI and ML-based decisions, to implement explainability requirements for significant algorithmic trading strategies, and to conduct regular algorithmic audits.[49] These obligations represent an important step towards AI accountability in the financial markets, but they are limited to intermediaries regulated by SEBI and do not cover the full range of AI applications in the financial sector.

The Insurance Regulatory and Development Authority of India (IRDAI) has also begun to examine the governance of AI in insurance, recognising both the potential of AI to improve underwriting efficiency and the risks of discriminatory pricing that can arise when AI systems use proxy variables that correlate with protected characteristics such as

[47]Reserve Bank of India (n 18).
[48]Reserve Bank of India (n 18).
[49]Securities and Exchange Board of India, Circular on Artificial Intelligence and Machine Learning Application by Market Intermediaries (SEBI 2019) <https://www.sebi.gov.in> accessed 18 April 2025.

caste, religion, or disability.[50] The liability exposure of insurance companies for discriminatory AI pricing decisions whether under the consumer protection framework, the equality provisions of the Constitution, or the specialised insurance regulatory framework remains an important unresolved question in Indian law.

The flash crash phenomenon where algorithmic trading systems interact in unforeseen ways, triggering a sudden and catastrophic market price movement presents another distinct AI liability issue in the financial services sector. Such events cause widespread harm to investors and can destabilise markets. The question of who bears liability for a flash crash caused by the interaction of multiple independent AI trading systems none of which was individually negligent is one of the most complex questions of AI liability that Indian financial law has yet to address. The application of the doctrine of absolute liability to financial AI systems that cause systemic market harm deserves serious consideration in the context of the reform of India's AI liability framework.

3.10 The Need for a Dedicated AI Liability Framework

It is shown in the analysis in this chapter that the current liability framework in India though not being totally irrelevant to AI-related harm is essentially insufficient in terms of overall coverage of the AI liability issues. The framework of negligence has been severely challenged by the inaccessibility of AI systems and the inability to prove causation and a violation of the standard of care. In high-risk AI systems, the absolute liability doctrine holds potential applicability, but has not been formally applied to the AI- specific context. The product liability framework of the CPA 2019 offers a partial foundation for AI product liability but leaves much to be desired.

It is accordingly arguable that India should come up with specific legislation on AI liability, either in isolation or as a subset of a broader AI regulation legislation. At least such a framework must: include clear attribution of liability between AI system developers, deployers and users, depending on their respective roles and the extent to which they can control AI behaviour; impose strict liability where harm is caused by high-risk AI systems; introduce a risk-based classification of AI systems akin to that

[50]Insurance Regulatory and Development Authority of India, Discussion Paper on Use of Artificial

Intelligence and Machine Learning by Insurance Intermediaries (IRDAI 2020).

employed by the EU AI Act; and introduce specific requirements of transparency and explanation on AI systems whose outputs impact the rights of any individual.

CHAPTER IV

INTELLECTUAL PROPERTY RIGHTS AND ARTIFICIAL INTELLIGENCE IN INDIA

4.1 Introduction

The set of issues and challenges surrounding Intellectual Property Rights (IPR) law is one of the most challenging and constantly changing in the realm of AI. The very basis of IP law that the attribution of temporary exclusive rights to creators and inventors drives the generation of socially valuable knowledge, expression and innovation is rooted in the premise that the concerned creator or inventor is a human being. The premises of IP law are called into doubt when AI systems provide outputs that are novel and creative in the legal sense literary works, artistic works, musical compositions, software and inventions that do not involve any meaningful contribution by humans in terms of creativity or inventiveness. This chapter focuses on AI and its impact on copyright laws and patent laws in India, relying on comparative jurisprudence and research on the topic to provide answers to critical questions posed by the current legal framework.

4.2 Copyright and AI-Generated Works

4.2.1 The Requirement of Human Authorship

The Copyright Act 1957 safeguards original literary, dramatic, musical and artistic works, along with cinematograph films and sound recordings.[51] The key to the copyright system is the idea of authorship: copyright in a piece of work first vests in the "author" of the piece, the definition of whom varies with the type of work. In the case of a literary, dramatic, musical, or artistic composition, the creator of the piece is the author. In the case of a computer-generated work, the Act states that the author is "the person who causes the work to be created".[52]

[51] Copyright Act 1957 (Act 14 of 1957), s 13.

[52]ibid, s 2(d)(vi).

In the historic case of Eastern Book Company v. D.B. Modak, the Supreme Court of India decided that copyright protection did not simply exist in mechanical compilation a human author had to exercise judgment, skill and creativity.[53] This rule is quite in line with the international rule of original expression, as it is based on the Berne Convention and the practice of the United States (Feist Publications, Inc. v. Rural Telephone Service Co.)[54] and other common law countries. The need to express human creativity poses serious challenges for AI-generated works: when an AI-based system composes a poem or a musical composition, with no significant human creative input, the work is not considered to meet the requirement of originality as it is currently perceived.

4.2.2 Computer-Generated Works under the Copyright Act 1957

The specific provision of the Copyright Act 1957 covering "computer-generated works" was brought into place by the Copyright (Amendment) Act 1994,[55] much earlier than the period of advanced generative AI. The provision was to cover the works that were created by computer programs which were used under human direction such as a computer-generated report created based on user-specified parameters or a graphic created by a design program based on the input of a user. When this happens, the "author" of the work that is created would generally be the programmer or the user who instructed the computer program.

What is not answered by Section 2(d)(vi) is the question of what happens when the work produced by the AI generator has no identifiable human author in any real sense that is, when an advanced generative AI system generates a work without particular human creative guidance. Does a corporation that educates and implements an AI system "cause a work to be created" within the meaning of Section 2(d)(vi)? And, in that case, does this interpretation push the notion of authorship beyond its limits? And otherwise, when there is no human or legal person who can properly be said to have caused the work to be created, does the work belong to the public domain?

The most justifiable reading of the text of Section 2(d)(vi) in the present-day AI context is that an entity that creates and implements a generative AI system can be considered the person who causes the work to be made, and that copyright in the AI-generated work

[53]Eastern Book Company v D.B. Modak (2008) 1 SCC 1.
[54]Feist Publications Inc v Rural Telephone Service Co 499 US 340 (1991).

[55]Copyright (Amendment) Act 1994 (Act 38 of 1994).

should be held by that entity. The benefit of this interpretation is that it retains the incentive regime of the copyright law to guarantee that investment in AI development is rewarded and is consistent with the principle that legal persons (such as corporations) can be authors and owners of copyright in some types of works. This interpretation has been criticised, however, on the view that it results in copyright monopolies without any human input to the creative process, which may unduly enrich a small number of large technology firms.

4.2.3 The Deepfake and AI-Generated Derivative Works Problem

Another similar and more pressing copyright issue is the use of generative AI systems trained on copyrighted content to produce new work which might or might not be infringing. Image generation systems and large language models are usually trained on massive text, image and other creative data, a large portion of which is copyrighted. The question of whether the training process itself constitutes a copyright violation is one that is hotly debated across several jurisdictions.

The Copyright Act 1957 gives right-holders the exclusive right to reproduce, translate, adapt and make other copies of their works.[56] The question of whether the ingestion of copyrighted material into an AI training dataset will be considered as reproduction under the meaning of the Act is a matter that Indian courts have not yet considered. Courts in the United States and Germany are now considering this issue in several high-profile cases against AI firms initiated by authors, publishers, and artists. The Indian Copyright Act lacks a fair use exception in line with the fair use doctrine in the US copyright law, and instead offers certain exceptions to fair dealing that are used to conduct research and to engage in personal study, criticism and newspaper reporting.[57] It is highly questionable whether the training of AI on copyrighted content is covered by any of these exceptions as per Indian law.

4.3 Patents and AI Inventorship

4.3.1 The Inventorship Requirement

[56]Copyright Act 1957 (Act 14 of 1957), s 14.
[57]ibid, s 52.

The patent law poses similar but different challenges. A patent can be granted under the Patents Act 1970 of an invention that is a new product or process involving an inventive step and capable of industrial application.[58] The Act vests the patent in the "true and first inventor" or his legal representative.[59] Similarly to the need for a human author in copyright law, the traditional assumption of patent law is that there must be a human inventor indeed, the very word "invention" has historically been perceived as a distinctively human intellectual accomplishment.

Indian courts and the Indian Patent Office have not yet dealt with the question of whether an AI system can be an "inventor" in the sense of the Patents Act 1970, although comparative jurisprudence can offer some guidance. The Federal Circuit Court of Appeals in Thaler v. Vidal decided that inventors under the Patent Act must be natural persons and that an AI system, the DABUS system created by Dr. Stephen Thaler, could not be referred to as an inventor.[60] The UK Supreme Court also reached the same decision in Thaler v. Comptroller-General of Patents, holding that an inventor under the Patents Act 1977 must be a person, and that the DABUS system, which was not a person, could not be an inventor.[61]

The reference to "the true and first inventor" in the Patents Act 1970 greatly implies that a person is the inventor in contemplation. The provisions of the Act on the issue of granting patents to the legal representatives of deceased inventors also testify to the paradigm case being human natural persons. Concerning the status of Indian patent law, therefore, one would assume that an AI system cannot be referred to as an inventor, and a patent application that would list an AI as the sole inventor would be rejected by the Indian Patent Office.

4.3.2 The Ownership Gap

The fact that AI systems are not considered to be inventors under the existing Indian patent law poses an acute practical issue: what of AI-generated inventions that are actually new and non-obvious inventions that would have been patentable had they been made by a human inventor? In the absence of an identifiable human inventor, the

[58]Patents Act 1970 (Act 39 of 1970), s 2(1)(j).
[59]ibid, s 6.
[60]Thaler v Vidal 43 F.4th 1207 (Fed Cir 2022).

[61]Thaler v Comptroller-General of Patents, Designs and Trade Marks [2023] UKSC 49.

invention cannot be patented and will remain in the public domain. Some scholars have justified this result by claiming that it is beneficial to the population because AI-generated innovations are made freely accessible, without the monopoly cost of patent protection.[62] Still others say it eliminates the patent motivation to invest in AI-assisted research and development, which could decrease the overall level of innovation.

The other solution would involve permitting the party that created and implemented the AI system to be named as the inventor of AI-generated inventions, on the pretext that the creativity of the AI system can be ascribed to the developer.[63] This would maintain the incentive regime of the patent law without raising the philosophically challenging question of AI legal personhood. It is a question to which the Indian Patent Office and the legislature have not yet given definite answers, and to which a solution is one of the key suggestions of this dissertation.

4.4 AI and Trade Secrets

In addition to copyright and patents, trade secret law has important implications for the governance of AI. AI systems especially the trained models of large language models, and other commercially valuable AI systems are hugely valuable intellectual property that their creators and holders do not want disclosed. In Indian law, trade secrets are safeguarded by the law of breach of confidence, a civil court remedy in the form of equitable relief, and the criminal provisions of the Indian Penal Code on theft and criminal breach of trust.[64] In India, there is no specific trade secrets law, as there is in the United States (the Defend Trade Secrets Act 2016) or the European Union (the Trade Secrets Directive 2016).

The protection of AI models as trade secrets poses a direct conflict with the principles of transparency and explainability that an adequate AI governance framework would likely have to introduce. When AI developers can avoid this transparency because their models are considered a trade secret, the victims of AI decisions might not be able to

[62]Ryan Abbott, 'I Think, Therefore I Invent: Creative Computers and the Future of Patent Law' (2016) 57 Boston College Law Review 1079, 1082.
[63]Nandan Kamath, Law Relating to Computers, Internet and E-Commerce (5th edn, Universal Law Publishing 2018) 145.

comprehend, object, or assert remedies to those decisions. This conflict between trade secrets and AI disclosure is one of the most difficult elements of AI governance design, and it is quite plausible that India should create a new law on trade secrets that specifically resolves this conflict by allowing some disclosure of AI systems to regulators and, in special circumstances, to affected parties.

4.5 Data Rights and AI Training Datasets

One last aspect of IPR and AI that should be discussed is the issue of data rights in particular, the legal status of the enormous datasets that AI systems are trained on. The data in AI training datasets can be a mix of publicly accessible data, licensed proprietary data and, in certain instances, unauthorised and unconsented data. The implications of AI training datasets for copyright and database rights are controversial.

The Copyright Act 1957 protects compilations of data as literary works, provided the selection and arrangement of the data reflects original creative expression.[65] However, a raw database of personal data such as photographs, text posts, or medical records used to train AI systems may not attract copyright protection if its compilation lacks the requisite originality. India does not have a sui generis database right of the kind that exists in the European Union, which protects the substantial investment in collecting and organising databases regardless of originality. This gap in India's IP framework may reduce the incentive to invest in high-quality AI training datasets and may leave data providers without adequate recourse when their data is used without permission to train AI systems.

4.6 International Comparative Approaches to AI and Intellectual Property

The intersection of AI and intellectual property has generated significant comparative jurisprudence and legislative activity across major jurisdictions. An examination of these comparative developments is important both for understanding the global legal landscape and for drawing lessons that can inform the reform of India's IP framework in the context of AI.

[65]Eastern Book Company v D.B. Modak (n 46).

The World Intellectual Property Organization (WIPO) has conducted a series of conversations on AI and IP, exploring the implications of AI for copyright, patents, trade marks, designs and trade secrets.[66] The WIPO process has revealed deep divergences of view among member states on fundamental questions such as whether AI systems should be accorded any form of legal personhood for IP purposes, whether AI-generated works should attract copyright protection, and whether the existing frameworks of copyright and patent law are adequate to incentivise investment in AI development. India has been an active participant in the WIPO process and has contributed its own positions on these questions, which broadly align with the view that IP protection for AI-generated works and inventions should be contingent on some form of human contribution.

In the United States, the Copyright Office has clarified that it will only register copyright in works that are the product of human authorship, and that works produced by machines without human creative intervention are not copyrightable.[67] The US approach thus closely mirrors the Indian position under the Eastern Book Company judgment. However, the US Copyright Office has also indicated that it may register copyright in AI-assisted works, where a human author makes sufficient creative choices in the use of AI tools. This nuanced position distinguishing between AI-generated and AI-assisted works may be a useful model for India to adopt through legislative amendment or administrative guidance.

In Australia, the Federal Court in Acohs Pty Ltd v Ucorp Pty Ltd held that a computer-generated work lacked an original human author and therefore could not attract copyright protection.[68] This decision aligned with the constitutional basis of Australian copyright law, which requires a human author, and has influenced the subsequent debate in Australia about how the copyright framework should be reformed to address AI- generated works. India's situation is analogous the copyright framework, as currently interpreted, requires human authorship and the Australian experience demonstrates the difficulty of extending copyright to purely AI-generated works through judicial interpretation alone, suggesting that legislative action will be necessary.

[66]World Intellectual Property Organization, WIPO Conversation on Intellectual Property and Artificial Intelligence: Third Session (WIPO 2020) WIPO/IP/AI/3/GE/20/1.
[67]US Copyright Office, Copyright and Artificial Intelligence: Part 1 – Digital Replicas (US Copyright Office 2023).
[68]Acohs Pty Ltd v Ucorp Pty Ltd [2012] FCAFC 16 (Australia).

The European Union, in the context of the AI Act and the broader revision of the EU intellectual property framework, has been considering how to address the IP implications of AI. The EU approach has focused on transparency requirements requiring AI providers to disclose when their systems have been trained on copyrighted works as well as on extending or clarifying text and data mining exceptions to copyright law to facilitate lawful AI training. These provisions have attracted significant controversy from rights- holders, who argue that they are inadequate compensation for the use of their works in AI training. India does not have a text and data mining exception to copyright, and the introduction of such an exception, with appropriate safeguards for rights-holders, may be a legislative option worth considering.

On patents, the comparative picture is broadly consistent: no major jurisdiction currently allows an AI system to be named as an inventor, and the trend in the jurisprudence is clearly towards requiring human inventorship. The critical question for India, as for other jurisdictions, is how to address the ownership gap for AI-generated inventions that would otherwise be patentable. India should consider following the approach suggested by some scholars of allowing the developer and deployer of the AI system to be treated as the inventor of AI-generated inventions, on the analogy of the "person who causes the work to be created" concept in copyright law.

CHAPTER V

DATA PROTECTION, PRIVACY AND THE REGULATION OF AI IN INDIA

5.1 Introduction

One of the most significant aspects of the AI governance issue is the connection between Artificial Intelligence and the right to privacy. AI systems are not passive data consumers, but active generators of new personal data via inference and prediction. A machine learning system that has been trained on browsing history can conclude that a person has a specific political behaviour, health issues, or sensitive attributes that they did not necessarily reveal themselves. A facial recognition system identifies faces in open areas without the knowledge or consent of the people. Predictive policing algorithms give people risk scores based on the history of their behaviour, virtually placing them under surveillance and pre-emptive investigation. Such abilities position AI at the heart of the modern battle to maintain human autonomy, dignity and freedom in the digital era.

The constitutional and statutory protection of privacy and data protection laws in India have witnessed a radical change over the past few years. This chapter evaluates that development most importantly the unanimous acknowledgment of privacy as a primary right in the Puttaswamy decision by the Supreme Court and the passage of the Digital Personal Data Protection Act 2023 and its suitability to the context of AI regulation. It recognises major discrepancies between the existing law and the requirements of AI accountability, and suggests certain changes.

5.2 Privacy as a Fundamental Right: The Puttaswamy Judgment

One of the most important constitutional pronouncements in the history of Indian law is the decision of the nine-judge bench of the Supreme Court in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India.[69] The nine-judge bench voted unanimously that the right to privacy was a fundamental right safeguarded by Article 21 of the Constitution of

[69]Justice K.S. Puttaswamy (Retd) v Union of India (n 11).

India, as part of the right to life and personal liberty, as well as by Articles 14 and 19, to the extent that they contradicted the prior decisions in Kharak Singh v. State of U.P.[70] and M.P. Sharma v. Satish Chandra.

The Puttaswamy decision describes a rich conception of privacy which includes informational privacy the right to control information about oneself. In his concurring opinion, Justice D.Y. Chandrachud (as he then was) found informational privacy to embrace the right to decide what information about one's personal life is shared, the right to avoid being monitored, and the right to be forgotten.[71] All these aspects of privacy have direct and significant implications for AI systems that handle large volumes of personal data, make detailed profiles of individuals, and implement facial recognition and other surveillance technologies. The Puttaswamy decision confirms the three-fold test of legality, necessity, and proportionality as applied to any state action that violates privacy and, by implication, that private actors who engage in processing personal data in a manner that violates privacy may also be subject to constitutional responsibility.

5.3 The Digital Personal Data Protection Act 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the first general law on the protection of personal data in India, adopted after a lengthy and controversial legislative history, which involved the withdrawal of the initial Personal Data Protection Bill 2019 in August 2022.[72] The DPDP Act provides a framework of protection of digital personal data, and establishes responsibilities on Data Fiduciaries (entities that decide on the purpose and means of processing personal data) and Data Processors (entities that process personal data on behalf of Data Fiduciaries).

The provisions of the DPDP Act are relevant to AI systems. The Act mandates that Data Fiduciaries must seek the free, specific, informed, unconditional and unambiguous consent of the Data Principal when processing their personal data, unless it qualifies as one of the listed legitimate uses.[73] This consent directive directly applies to AI systems that process personal information such as the information used to train AI models, information processed by AI systems in offering personalised services, and information

[70]Kharak Singh v State of U.P. AIR 1963 SC 1295.
[71]Justice K.S. Puttaswamy (Retd) v Union of India (n 11), para 181 (per Chandrachud J).
[72]Digital Personal Data Protection Act 2023 (Act 22 of 2023).

[73]ibid, s 7.

produced by AI inference and profiling. The exceptions of the Act on legitimate uses, such as processing to comply with any law, employment-related processing and processing to fulfil reasonable purposes as set forth by the government, are however broadly formulated and can be used to greatly weaken the consent requirement in AI cases.

The Data Principals in the DPDP Act are also granted a set of rights: the right to access information on their personal data, the right to correct and erase their personal data, the right to grieve against Data Fiduciaries, and the right to have their rights exercised by another person on their behalf in case of incapacity or death.[74] These rights signify a major breakthrough in data protection in India. The DPDP Act however conspicuously does not address a number of AI-specific rights that international best practice such as the GDPR in the EU would afford: the right to an explanation of automated decisions is absent, there are no express prohibitions on automated profiling, and no compulsory human review requirement of AI systems making consequential decisions about individuals. This exclusion stands out as a critical lapse in the suitability of the Act as an instrument of AI regulation.

5.3.1 Significant Data Fiduciaries

The DPDP Act provides the category of Significant Data Fiduciary (SDF) Data Fiduciaries which may be designated so by government in view of the amount and sensitivity of the personal data they handle, the potential harm to Data Principals, the considerations of national security and national order, and their possible effects on sovereignty and integrity of India.[75] SDFs are required to comply with further requirements, such as appointing a Data Protection Officer, hiring an independent data auditor, and conducting Data Protection Impact Assessments. The SDF category is likely to have important applicability to the governance of AI: AI systems, including the financial AI system, the healthcare AI system, and the facial recognition database, are large-scale and may store sensitive personal information, meaning that they can be classified as SDFs and governed more rigorously.

[74] ibid, ss 11–14.
[75] ibid, s 10.

5.4 Facial Recognition Technology: Privacy and Discrimination Concerns

Facial recognition technology (FRT) takes an unprecedented front seat among the AI applications that threaten privacy rights the most. FRT makes it possible to identify or verify people based on their facial biometrics automatically, making surveillance at scale and discreetly possible. In India, FRT has been implemented by many state police forces to identify criminals in large crowds of people and during protests, at airports to check on passengers, and by other government departments to verify identity and control access.[76] The Delhi Police is said to have one of the biggest facial recognition databases in the world.

FRT brings up significant privacy issues at many levels. First, it allows sustained, massive covert surveillance of people in public areas without either their knowledge or consent, which is directly in conflict with the informational privacy aspect of the right to privacy identified in Puttaswamy. Second, many works have reported considerable accuracy differences in FRT systems, where women, darker-skinned people, and older people commit more errors, which are of significant concern due to the potential of discriminatory effects implicating the fundamental right of equality under Article 14 of the Constitution.[77] Third, FRT data is sensitive biometric data which, in case of breach or misuse, cannot be remedied unlike a password, an individual cannot change his or her face.

The Aadhaar Act 2016 that regulates the biometric identity system in India has certain limitations to the sharing and usage of biometrics data.[78] Special provisions that cover the processing of sensitive personal data, including biometric data, are also present in the DPDP Act 2023.[79] But neither law is sufficient to govern the use of FRT by the police or other government bodies. India is in dire need of a particular set of laws regarding facial recognition technology that outlines specific terms of use, control measures, accuracy requirements, and remedies for victims of misidentification.

---

[76]Internet Freedom Foundation, Facial Recognition Technology: Its Uses, Risks and Recommended Reforms (IFF 2022) <https://internetfreedom.in/facial-recognition-technology/> accessed 18 April 2025.
[77]Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77.
[78]Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (Act 18 of 2016), s 29.
[79]Digital Personal Data Protection Act 2023 (Act 22 of 2023), s 2(t).

5.5 Algorithmic Decision-Making and the Right to Explanation

Consequential decisions regarding individuals in the form of credit decisions, insurance pricing, employment screening, bail and sentencing recommendations, benefits eligibility are increasingly being made or assisted by AI systems in ways that can have far-reaching impact on the life opportunities and possibilities of individuals. In cases where opaque algorithmic systems make these decisions, individuals may not be in a position to comprehend why a decision about them was arrived at, challenge a wrong or discriminatory decision, or seek effective redress against unfair treatment.[80] This obscurity of AI decision-making poses a direct challenge to the rule of law and the principles of procedural fairness and natural justice that form the core of the Indian constitutional order.

Article 22 of the GDPR of the European Union deals with this issue by providing people with the right not to be subjected to automated processing that results in material consequences for them, together with the right to obtain information about the basis of the decision and to challenge it.[81] No similar provision is included in the DPDP Act 2023 of India, which is an important omission that can be considered one of the most severe gaps in the AI governance framework in India. The principles of natural justice developed by courts in India to restrict administrative decision-making the right to be heard and the rule against bias have not been generalised to algorithmic decision-making, and it is not clear how well they can be applied in the AI context without legislative direction.[82]

5.6 Algorithmic Bias and Discrimination

The algorithmic bias the propensity of AI technologies trained on historical data to reproduce, increase, or even create discriminating patterns is a severe danger to equality and non-discrimination in the Indian context. The results of AI systems used in credit, employment, healthcare and criminal justice determinations can be systematically adverse to already-marginalised groups scheduled castes, scheduled tribes, women, persons with disabilities, religious minorities as they learn and reproduce the historically biased

[80] Pasquale (n 29) 8.
[81] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) [2016] OJ L 119/1, art 22.
[82] Maneka Gandhi v Union of India AIR 1978 SC 597.

patterns they are trained on.[83] The threat of AI to reproduce and solidify social inequalities, apparently in a neutral and objective way, is particularly acute in a country with such a rich history of social inequality and discrimination.[84]

In the Indian constitutional system, the constitutional right to equality (under Article 14) and non-discrimination (under Article 15) and right to equality of opportunity (under Article 16) are fundamental rights that give a constitutional foundation to an appeal against discriminatory AI decisions. But the extension of these constitutional guarantees to algorithmic discrimination especially by non-governmental actors must be legislatively applied, and the DPDP Act 2023 does not make any explicit reference to algorithmic discrimination. Creating certain anti-discrimination clauses that could be used to regulate the AI decision-making systems is an obligatory aspect of a comprehensive Indian AI regulation system.

5.7 AI and the Right to Be Forgotten

The right to be forgotten the right of an individual to have personal information about them erased from digital systems, particularly from search engines and online databases has gained significant international recognition as an aspect of the right to privacy in the digital age. The European Court of Justice in Google Spain SL v. Agencia Española de Protección de Datos established the right to erasure as a component of the European data protection framework.[85] Article 17 of the GDPR subsequently codified this right, allowing individuals to request the erasure of their personal data in a range of circumstances, including when the data is no longer necessary for the purpose for which it was collected, when the individual withdraws consent, or when the data has been unlawfully processed.[86]

The DPDP Act 2023 of India provides a right to erasure of personal data under Section 13, which allows Data Principals to request Data Fiduciaries to erase their personal data

[83]Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (St Martin's Press 2018) 5.
[84]Mireille Hildebrandt and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73 Modern Law Review 428, 441.
[85]Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (C-131/12) [2014] ECLI:EU:C:2014:317.
[86]Regulation (EU) 2016/679 (n 73), art 17.

and to cease further disclosure.[87] This right is subject to certain limitations, including where the retention of data is necessary for compliance with any law or for the fulfilment of the purpose for which the data was collected. The right to erasure under the DPDP Act is thus a limited right, and its application in the context of AI systems raises complex challenges that the Act does not adequately address.

The most significant challenge is the technical impossibility or extreme difficulty of implementing the right to erasure in relation to AI systems that have been trained on personal data. Once personal data has been incorporated into the training of a machine learning model, it is not straightforwardly possible to "erase" that data from the model the data may have contributed to the millions or billions of parameters that define the model's behaviour, without being identifiably present in any discrete form. The concept of "machine unlearning" the development of technical methods to remove the influence of specific training data from trained AI models is an active area of AI safety research, but there are as yet no widely accepted standardised methods for implementing machine unlearning at scale.

The implications of this technical challenge for the DPDP Act's right to erasure are profound. If a Data Principal requests erasure of their personal data from a Data Fiduciary that has used their data to train an AI model, the Data Fiduciary may be technically unable to comply fully with the erasure request. The Act does not address this scenario, leaving open the question of what obligations a Data Fiduciary bears when technical compliance with an erasure request is not possible. India should consider amending the DPDP Act to specifically address the right to erasure in the AI training data context, including obligations of transparency about the use of personal data in AI training, the need to obtain specific consent for the use of personal data in AI training, and technical and procedural obligations where full erasure is not possible.

[87]Digital Personal Data Protection Act 2023 (Act 22 of 2023), s 13.

CHAPTER VI

AI, CYBERCRIME AND THE CRIMINAL JUSTICE SYSTEM IN INDIA

6.1 Introduction

The future of crime and criminal justice in India is changing due to Artificial Intelligence, which provokes multiple legal concerns that are both deep and urgent. On the one hand, criminal actors are weaponising AI to perpetrate new types of cybercrime deepfakes committed in fraud, defamation, and non-consensual intimate image abuse; AI-based phishing and social engineering attacks; AI-generated misinformation and propaganda; and AI-enabled child sexual abuse. Meanwhile, the state is deploying AI as a crime control and criminal justice tool predictive policing, AI-assisted evidence analysis, facial recognition to identify suspects, and even AI-assisted sentencing suggestions. Both of these sides create great legal issues to the criminal law system in India, which was not programmed to handle AI.

6.2 Deepfakes and AI-Generated Harmful Content

One of the most frightening uses of generative AI in the criminal realm is deepfakes artificial media that are AI-generated and which look and sound convincingly like real individuals saying or doing things that they did not actually say or do. The technology of deepfaking has become disastrously easy to use and allows producing believable fake videos and audio recordings without much technical know-how, through the usage of deep learning algorithms like Generative Adversarial Networks (GANs). The possible negative uses of deepfakes are numerous: they can be employed to slander someone by presenting them in an untrue scenario; to commit fraud by posing as a business executive, family member or government official; to produce non-consensual intimate imagery (NCII) against women and girls; and to propagate political disinformation.[88]

[88]Robert Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and

National Security' (2019) 107 California Law Review 1753, 1758.

The current criminal law system in India offers partial, yet insufficient solutions to deepfake harm. Deepfakes involving defamation can be liable under the Indian Penal Code 1860, Sections 499 and 500 (defamation), and deepfakes involving impersonating others to commit fraud can be liable under Sections 419 (cheating by personation) and 420 (cheating and dishonestly inducing delivery of property).[8990] Intimate deepfakes involving no consent can be liable under Section 354C of the IPC (voyeurism), but the correspondence between the provision and AI-generated synthetic images is not a perfect fit, as it was intended to encompass the surreptitious recording of real individuals and not AI-generated synthetic imagery.[91] Section 67 (obscenity) and Section 67A (sexually explicit content) of the IT Act 2000 may apply to certain deepfakes, and Sections 66C (identity theft) and 66D (cheating by personation using computer resources) may apply to identity-based deepfake fraud.[9293]

Nevertheless, the current provisions are not comprehensive enough to tackle all the harms related to deepfakes. No particular crime of making or sharing non-consensual deepfake intimate images is present, which leaves an entire category of victims most of whom are women without sufficient legal redress. The IT Act has a wide set of obscenity provisions that are ill-defined and may include legitimate artistic or journalistic applications of deepfake technology. India is in need of a specific law that would cover the creation and spread of deepfakes in a way that would unambiguously define the crime, establish a system of proportional punishment, and offer a faster takedown system without sacrificing the right to legitimate satirical and artistic applications of synthetic media.[94]

6.3 AI-Enabled Cybercrime

In addition to deepfakes, AI is facilitating a wide scope of cybercrime that Indian criminal laws are unable adequately to deal with. Machine learning-based phishing attacks that incorporate AI to create highly personalised and persuasive fraud messages, replicating the writing style of trusted contacts, are becoming more advanced and challenging to recognise. Automated botnets powered by AI may be used to organise distributed denial

[89]Indian Penal Code 1860 (Act 45 of 1860), ss 499, 500.
[90]ibid, ss 419, 420.
[91]ibid, s 354C.
[92]Information Technology Act 2000 (Act 21 of 2000), ss 67, 67A.
[93]ibid, ss 66C, 66D.

[94]Pavan Duggal, Cyberlaw: The Indian Perspective (2nd edn, Saakshar Law Publications 2014) 210.

of service (DDoS) attacks, disseminate disinformation on a large scale, and manipulate social media. AI-based vishing (voice phishing) attacks utilise AI voice-cloning technology to make fraudulent phone calls that impersonate bank managers or government officials to obtain sensitive information or payments.

In theory, these AI-enhanced cybercrime acts can be prosecuted under the current provisions of the IT Act 2000 especially Section 66 (computer-related offences),[95] Section 66C (identity theft), Section 66D (cheating by personation), and the provisions of the Penal Code on fraud. Section 66F on cyberterrorism may also be applicable in extreme cases.[96] But the attribution problem of locating and prosecuting the human operators of AI-enabled cybercrime tools is incredibly complicated, especially when tools are used across international borders. The evidentiary issues of establishing criminality in Indian courts such as the admissibility and reliability of electronic evidence are magnified in AI cybercrime cases by the technical nature of the evidence and the opacity of AI systems.[97]

6.4 AI in the Criminal Justice System: Predictive Policing and Risk Assessment

The implementation of AI in the criminal justice system presents issues that are at least as grave as those posed by AI-enabled crime. When the state relies on AI to make judgements about those under surveillance, who is stopped and frisked, who is arrested, who is denied bail, and how many years a person spends in prison, the possibility of AI bias and error leading to grave injustice is great. The application of AI in such high-stakes situations implicates numerous fundamental rights: the right to liberty (Article 21), the right to equality (Article 14), the right against self-incrimination (Article 20(3)), the right to a fair trial, and the right against discrimination.[98]

Predictive policing systems apply machine learning algorithms to define high-risk locations, times, or individuals based on past crime data, producing individual risk scores that are supposed to forecast the probability of future criminal behaviour. These systems

[95] Information Technology Act 2000 (Act 21 of 2000), s 66.
[96] ibid, s 66F.
[97] Pankaj Mishra, 'Algorithmic Justice: Rethinking Criminal Law in the Age of AI' (2023) 45 Journal of Law and Technology 23, 28.
[98] Selvi v State of Karnataka (2010) 7 SCC 263.

have been implemented in one form or another by police forces in large Indian cities, but have been controversial and opaque in their application. It has been criticised that predictive policing systems trained on past crime data merely recreate historical over-policing trends, whereby already-targeted communities are disproportionately subject to police scrutiny, resulting in more crime being recorded, which in turn feeds the predictive policing training data that justifies further targeting.[99]

The international experience with predictive policing and AI-based risk assessment provides important cautionary lessons for India. In the United States, the COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) risk assessment system, used in several states to inform bail and sentencing decisions, was found by investigative journalists at ProPublica to have been twice as likely to incorrectly flag Black defendants as higher risk compared to white defendants. While the methodology of the ProPublica analysis was disputed, the controversy highlighted the profound risks of algorithmic bias in the criminal justice context. The state of Wisconsin's use of COMPAS scores in sentencing was challenged in the courts, but the Supreme Court of Wisconsin ultimately declined to hold that the use of algorithmic risk assessments in sentencing violated the defendant's constitutional rights, although it required that defendants be informed of the limitations of such assessments and be given the opportunity to challenge them.

Through a series of rulings, the Supreme Court of India has determined that the right to personal liberty under Article 21 must be supported by procedural fairness, that reasons why liberty is being deprived or why bail is not provided must be communicated to the detained individual, and that there must be effective remedies to illegal detention.[100] Implementing these principles in the context of AI risk assessment would require, at a minimum, that defendants be informed when an AI risk assessment has been used in making decisions about their freedom, that they have access to information about how the AI system functions and what contributed to their risk score, and that they be permitted to challenge the assessment of the AI before a competent authority.

[99]Kate Crawford, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence (Yale University Press 2021) 97.

The transparency and accountability requirements for AI in criminal justice are thus not merely policy preferences they are constitutional imperatives. The failure of Indian law to provide such requirements in the context of AI-based risk assessment and predictive policing represents a serious constitutional deficit that requires urgent legislative remedy.

6.5 AI-Generated Evidence

There are complicated issues concerning the admissibility, reliability and probative value of AI-generated or AI-analysed evidence used in a criminal process. Electronic records are admissible evidence under the Indian Evidence Act 1872 (with digital amendments also following the IT Act) provided that a certificate under Section 65B of the Evidence Act has been produced by a person in charge of the working of the computer that created the electronic record.[101] The Supreme Court addressed the certification requirement in Anvar P.V. v. P.K. Basheer[102] and later in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,[103] where it was ruled that the Section 65B certificate is a condition precedent to the admissibility of electronic records as secondary evidence.

AI-generated evidence including transcripts created using AI speech recognition, images or videos created using AI enhancement algorithms, or reports created using AI forensic analysis tools has special admissibility issues over and above those pertaining to regular electronic evidence. The output of an AI system can be unreliable when the accuracy of the system in the situation under consideration has not been validated, when it has been trained on non-representative data, or when the system itself has been tampered with. The explainability gap the inability to provide a human-understandable account of why an AI system gave a specific output offloads courts with the task of determining the reliability of AI evidence according to the traditional frameworks of expert analysis and its foundation and methodology. The newly adopted Bharatiya Sakshya Adhiniyam 2023 provides a revised framework for electronic evidence but does not specifically address the particular challenges of AI-generated evidence.[104] Specific evidentiary rules for AI- generated evidence in criminal trials are urgently required.

[101] Indian Evidence Act 1872 (Act 1 of 1872), s 65B.
[102] Anvar P.V. v P.K. Basheer (2014) 10 SCC 473.
[103] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

[104]Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023), s 61.

6.6 AI-Generated Child Sexual Abuse Material

One of the most shocking uses of generative AI is its deployment to produce child sexual abuse material (CSAM). Image and video creation systems based on generative AI can create extremely realistic synthetic sexual images of children without a real child being directly involved in the creation of the imagery. Although this kind of imagery does not involve the direct exploitation of a real child, it desensitises viewers to child sexual abuse, may trigger the desire to acquire real CSAM and can be used in grooming children.

The Protection of Children from Sexual Offences Act, 2012 (POCSO Act) and the IT Act in India have provisions regarding CSAM.[105] Nonetheless, the definition of child sexual abuse content in the POCSO Act is devoted to the depictions of actual children, and it is unclear whether AI-generated synthetic CSAM falls within the definition unambiguously. Section 67B of the IT Act, which criminalises the publication or transmission of any material that portrays children engaging in sexually explicit acts, is general enough to potentially include AI-generated synthetic materials, although this has not been definitively determined by the Indian courts.[106] India must make sure, by interpretation or by legislative amendment, that AI-created CSAM is explicitly forbidden and harshly punishable, whether or not the creation involved any actual child.

[105]Protection of Children from Sexual Offences Act 2012 (Act 32 of 2012).

[106]Information Technology Act 2000 (Act 21 of 2000), s 67B.

CHAPTER VII

TOWARDS A REGULATORY FRAMEWORK FOR AI GOVERNANCE IN INDIA

7.1 Introduction

Throughout the previous chapters, it has been recorded, in various fields of law, that the current legal system in India is totally inadequate to regulate the creation and use of Artificial Intelligence. The liability regulations are unclear and do not reflect AI peculiarities; intellectual property law contains significant gaps on AI authorship and inventorship; data protection regulation is not designed to capture AI-specific risks such as algorithmic decision-making and profiling; criminal law is ineffective against AI- related crimes and AI-assisted injuries; and the overall regulatory framework is inconsistent, reactive, and lacks the institutional capability to oversee, assess, and respond to the fast-evolving AI ecosystem. This chapter provides a synthesis of the results of the analysis conducted above and sets out a set of recommendations to develop a comprehensive AI governance framework in India.

7.2 Mapping the Existing Regulatory Landscape

The current AI-relevant regulatory environment in India is defined by the absence of coherence, sector-specificity, and predominantly voluntary or aspirational tools. Topping the list is NITI Aayog, which has published a set of policy papers describing the Government's vision of AI and its principles, such as the National Strategy on Artificial Intelligence (2018), the reports on Responsible AI for All (2021), and the Cloud and AI Infrastructure Policy (2023).[107][108] These are documents that express significant values such as inclusiveness, safety, transparency, accountability but they are not binding and do not create binding obligations or institutional mechanisms.

[107] NITI Aayog, National Strategy for Artificial Intelligence (n 4).

[108]NITI Aayog, Cloud & AI Infrastructure Policy (Government of India 2023).

India has been most active at the sectoral level with regards to AI governance. The RBI Digital Lending Guidelines and its deliberations on AI risk in the financial sector have established a few expectations about responsible AI application in financial institutions. SEBI has provided advice on how market intermediaries use AI and machine learning, and mandates policies, disclosures, and audit trails.[109] IRDAI has already started to analyse AI in insurance, and the National Health Authority has created the Digital Health Blueprint that reflects on the usage of AI in healthcare.

The Information Technology (Amendment) Rules 2023, which created a category of "significant social media intermediaries" with increased responsibility, have AI governance implications in the area of AI-generated content moderation and algorithmic curation, though they are not explicitly aimed at AI governance. The Expert Committee on AI (2023) of MeitY has suggested an AI governance framework, grounded on the principles of fairness, accountability, transparency, ethics and inclusion (FATE), but this framework is at the proposal stage.

7.3 Principles for an Indian AI Governance Framework

The AI governance model in India should be based on a consistent body of values that not only embodies universal values human dignity, equality, fairness, accountability, and the rule of law but also reflects India and its particular constitutional obligations and developmental goals. Based on the comparative analysis in the previous chapters and on the constitutional framework of India, this dissertation suggests the following principles as the basis of an Indian AI governance framework.

7.3.1 Human-Centred and Rights-Based Approach

The Indian AI governance model should put human beings and their rights and welfare at the centre of AI governance. The deployment, development, and design of AI systems must be in a manner that does not violate the basic rights contained in Part III of the Constitution of India, such as the right to equality (Article 14), the right to freedom of expression (Article 19), and the right to life and personal liberty (Article 21). Any limitation of such rights by AI systems should be in compliance with the constitutional

[109]Securities and Exchange Board of India (n 42).

requirements of legality, necessity, and proportionality set out in the Puttaswamy judgment.[110]

7.3.2 Risk-Based and Proportionate Regulation

The risks of AI applications are not equal. A regulatory framework that imposes similar demands on a low-risk AI application (such as a spell-checking application or a product recommendation algorithm) as it does on a high-risk application (such as a medical diagnostic system, an autonomous vehicle, or a surveillance tool used by law enforcement) would be both disproportional and costly. The AI governance framework in India must be risk-based, similar to the EU AI Act, that calibrates regulatory requirements according to the degree and likelihood of possible harm.[111]

7.3.3 Transparency and Explainability

Accountability in AI governance requires preconditions of meaningfulness and explainability. Affected persons under AI decision-making should be told that an AI system was used to make a decision about them, have access to the main factors which contributed to the decision, and have a meaningful chance to challenge the decision. To exercise their supervisory role, regulators and oversight bodies should have access to the design, training data, and evaluation results of AI systems. The black box issue the opaqueness of machine learning models is not technically unsolvable in most applications: in most settings, explainable AI (XAI) methods can give human- understandable explanations of AI decisions. The AI governance framework in India must require more or less transparency, depending on the risk associated with the AI application and the importance of the decisions being made.

7.3.4 Accountability and Oversight

Accountability demands that identifiable human or legal persons are responsible for the behaviour of AI systems, and can face civil, criminal or regulatory accountability in case the AI systems cause harm or infringe rights. The AI governance system in India should also explicitly allocate the accountability roles along the AI value chain to developers, deployers and users of AI systems in a manner that generates significant incentives to behave responsibly. It needs not only clear rules of liability (as outlined in Chapter III)

[110] Justice K.S. Puttaswamy (Retd) v Union of India (n 11).

[111]Regulation (EU) 2024/1689 (n 15), Recital 14.

but also institutional accountability: independent AI regulators with sufficient powers and expertise, obligatory incident reporting and auditing, and civil society and parliamentary monitoring of AI in the public sector.

7.3.5 Inclusion and Non-Discrimination

The principle of inclusion and non-discrimination is especially relevant to the AI governance scenario in India, which is incredibly diverse with regard to language, caste, religion, geography, and socioeconomic status. AI systems that are developed based on data that fails to effectively represent the diverse population of India will inherently perform poorly with underrepresented populations. Artificial intelligence that continues past patterns of discrimination will widen social disparities. A system of AI governance in India should demand that AI developers and deployers evaluate and tackle bias and discrimination within their systems and should enable the affected communities especially those who are historically marginalised to report and demand redress against discriminatory AI actions.

7.4 Recommended Legal and Regulatory Reforms

This dissertation suggests the following specific legislative, institutional, and policy proposals to develop a comprehensive AI governance framework in India based on the analysis in the preceding chapters and the principles presented above.

7.4.1 Enactment of an AI Governance Act

India ought to introduce a broad horizontal AI Governance Act that would bring about a common framework in the development, deployment, and regulation of AI systems in all sectors. Modelled in its structure on the EU AI Act but adapted to India's constitutional and developmental context, the AI Governance Act should: (i) adopt a risk-based classification of AI systems into prohibited, high-risk, and general-purpose categories; (ii) establish mandatory requirements for high-risk AI systems including conformity assessments, technical documentation, transparency to users, human oversight mechanisms, and registration in a public AI registry; (iii) prohibit AI applications that are incompatible with fundamental rights, including AI social scoring, covert subliminal manipulation, and real-time remote biometric identification in public spaces for law enforcement purposes except with prior judicial authorisation; (iv) establish a liability

framework that allocates responsibility for AI-caused harm among developers, deployers, and operators based on their respective roles and control; (v) grant individuals rights including the right to explanation for automated decisions, the right to human review of consequential AI decisions, and the right to contest AI decisions that affect their rights or interests.

The AI Governance Act should also include provisions dealing with the cross-border dimension of AI governance. Many AI systems used in India are developed or operated by entities outside India, and the governance framework must have extraterritorial effect applying to any entity that deploys an AI system that affects persons in India, regardless of where the entity is based. This approach is consistent with the digital markets governance strategies adopted by the EU in the GDPR and the AI Act, and is necessary to ensure that the protections of the AI Governance Act cannot be circumvented by offshoring AI development or operation.[112]

7.4.2 Amendment of the DPDP Act to Address AI-Specific Issues

The Digital Personal Data Protection Act 2023 needs to be revised so that it covers AI-specific data protection issues that the Act does not currently address. Particularly, the amended Act should: (i) acknowledge a right against being subjected to decisions based entirely on automated processing that have serious consequences on the Data Principal, similar to Article 22 of the EU GDPR; (ii) make Data Fiduciaries who apply AI systems in automated decision-making liable to provide meaningful explanations of the basis of such decisions; (iii) establish specific safeguards for the use of personal data in AI training, including clear consent requirements and obligations in relation to the right to erasure of training data; and (iv) establish mandatory data protection impact assessment obligations for the deployment of high-risk AI systems that process personal data.

7.4.3 Amendment of Intellectual Property Laws

The Copyright Act 1957 and Patents Act 1970 should be revised to deal with the legal position of AI-generated works and inventions. In the case of copyright, the amendment must specify that AI-generated works works created by AI without any meaningful human creative input should have a reduced term of protection compared to those created

[112]Ajay Agrawal, Joshua Gans and Avi Goldfarb, Prediction Machines: The Simple Economics of Artificial

Intelligence (Harvard Business Review Press 2018) 180.

by human authors (say 25 years since creation as compared to the life of the author plus 60 years), and that the copyright in such works shall accrue to the person who developed and deployed the AI system. In the case of patents, the amendment must provide that the human or legal entity that creates an AI system is considered as the inventor of inventions created by that AI system, as long as the intellectual contribution of the entity to the inventive process is documented, and that inventions created by an AI system that are truly novel and non-obvious may be patented.

7.4.4 Criminal Law Reforms

The Indian Penal Code and Information Technology Act 2000 should be revised to cover AI-enabled offences in a holistic manner. In particular, India ought to enact specific provisions criminalising: (i) the creation and sharing of non-consensual deepfake intimate content, to which greater punishments should be applied where the victim is a minor; (ii) the creation and sharing of any AI-generated content that constitutes child sexual abuse material, whether or not actual children have been depicted; (iii) the use of AI to spread intentional political disinformation during elections or in matters of national security. The newly adopted Bharatiya Sakshya Adhiniyam 2023 needs to be complemented with specific rules that regulate the admissibility, disclosure and assessment of AI-generated and AI-analysed evidence in court.

7.4.5 Establishment of an AI Regulatory Authority

Any AI governance framework can only be implemented effectively if there is a regulatory authority that is independent, well-resourced, and technologically competent. The proposed AI Governance Act should provide for the creation of an AI Regulatory Authority (AIRA) with statutory powers to: (i) register and oversee high-risk AI systems;
(ii) audit and investigate AI systems used in high-risk applications; (iii) provide binding guidance and technical standards on AI safety, transparency, and accountability; (iv) investigate and sanction violations of the AI Governance Act and related legislation; and (v) participate in international forums on AI governance and coordinate India's engagement with global AI standards bodies.

The AIRA must be mandated to engage in consultation with a multi-stakeholder advisory council, which contains representatives of civil society, academia, the AI industry, and affected communities, to make sure that its action is informed by diverse perspectives and

held accountable to the population it serves. The independence of the AIRA from both governmental and commercial interests is essential to its credibility and effectiveness as an AI regulator. India should study the governance and operational models of well-functioning independent regulatory bodies such as the Competition Commission of India, the Securities and Exchange Board of India, and the Telecom Regulatory Authority of India in designing the institutional structure and independence mechanisms of the AIRA.[113]

7.4.6 Investment in AI Safety Research and Public Education

Responsible AI governance does not require only legal and regulatory reform, though it is important. India ought to invest heavily in AI safety research the technical research of how to ensure that AI systems act safely, reliably, and in line with human values and in multidisciplinary AI ethics research that studies the social, economic, and ethical impacts of AI in the Indian context. India is also encouraged to invest in the AI literacy of judges, government employees, law enforcement agencies, and the general population, so that the AI governance framework of India is comprehended, honoured, and put into practice. The institutions of world-class technological status in India such as the IITs, IISc and others should be given specific funding and set up AI safety and AI ethics research centres. Moreover, MeitY ought to establish a national AI education framework that familiarises AI concepts, possibilities, and threats to the education system at every level, starting at the primary school level and up to professional education.

7.5 Balancing Innovation and Regulation

The prevailing counterargument to broad regulation of AI is that it will suppress innovation and make India less competitive in the worldwide AI industry. This is an objection which should be seriously considered. India boasts a real competitive advantage in AI a large source of technical talent, a rich and diverse data base, an active start-up culture, and governmental investment in AI. Ineffective regulation may actually subject small and medium AI firms to excessive compliance expenses, reduce the rate of AI uptake in socially valuable applications, and push AI creation to less regulated

[113]Gary Marcus and Ernest Davis, Rebooting AI: Building Artificial Intelligence We Can Trust (Pantheon 2019) 190.

jurisdictions. Such issues are valid and have to be incorporated in the architecture of any Indian AI governance system.

The experience of other jurisdictions points to the fact, though, that regulation designed well does not necessarily conflict with AI innovation. The GDPR of the EU which many had anticipated would throttle the digital economy in Europe has actually contributed to instilling trust in digital services and establishing a level playing field in the regulatory arena. The EU AI Act, which follows a risk-based approach making high-risk applications alone subject to heavy obligations, is clearly designed to enable positive AI innovation and safeguard against harm. India can follow a similar path by implementing a proportional, risk-based structure that will provide surety to responsible innovators and safeguards people and society against AI-enabled harm. In fact, an appropriate regulatory framework can itself act as an impetus to innovation by establishing a set of rules of the road, establishing trust in AI systems among the population, and offering AI companies the legal confidence they require to draw investment.

The peculiarities of Indian development should also be considered in the framework of AI governance. India, being a nation where AI has tremendous potential to solve urgent social issues in healthcare, agriculture, education and public service delivery, cannot afford the purely precautionary view of regulating AI, which puts more emphasis on reducing risk over the positive outcomes of AI adoption. A responsible innovation model that proactively supports the positive use of AI and deals with risks by calibrated regulation accordingly is the best model to address the developmental level of India and its goals. This balance should be clearly considered in the proposed AI Governance Act, which is to be supplemented by sector-specific regulatory guidance from the AIRA as well as by the already-existing sectoral regulators.

7.6 India's Path Forward: A Comparative Assessment

A comparative assessment of India's position in the global AI governance landscape reveals both significant deficits and important opportunities. On the one hand, India is the last major economy without any binding legal framework specifically addressing AI. The EU has the AI Act, China has a comprehensive set of application-specific AI regulations, the UK has a principles-based governance framework backed by sectoral regulators and the AI Safety Institute, and even some developing countries in Africa and Southeast Asia

have adopted or are developing national AI governance frameworks. India's regulatory gap is increasingly anomalous in the global landscape and creates risks not only for individuals and communities who are subject to the harms of ungoverned AI, but also for India's AI industry itself, which operates in the absence of legal certainty and faces the risk of market access barriers as other jurisdictions introduce adequacy requirements for trading partners.

On the other hand, India has several significant advantages in the development of its AI governance framework. As a relative latecomer to binding AI legislation, India can benefit from the experience of the EU AI Act learning from its implementation challenges, its areas of ambiguity, and the critiques that have been directed at it in designing a governance framework that is better adapted to India's specific conditions. India's massive and diverse AI deployment context spanning agriculture, public health, financial inclusion, judicial administration, and public security provides a rich empirical base for understanding the actual risks and benefits of AI deployment in developing country conditions, an understanding that is largely absent from the developed-country regulatory frameworks that have driven global AI governance discourse to date.

India's constitutional framework also provides a distinctive normative foundation for AI governance. The Indian Constitution's comprehensive bill of rights, its commitment to social justice and affirmative action, its directive principles addressing poverty, inequality and access to education and work, and its strong tradition of public interest litigation which has enabled civil society to use the courts to enforce constitutional norms against powerful actors together constitute a distinctive and potent foundation for rights- protective AI governance. The challenge is to translate these constitutional resources into specific legislative and institutional mechanisms that provide effective governance of AI in the Indian context.

India should also leverage its international relationships in designing its AI governance framework. India is a founding member of the Global Partnership on AI (GPAI), a multi-stakeholder international organisation dedicated to responsible AI development. It has engaged actively in the OECD, G20, and UNESCO processes on AI governance. It has bilateral AI cooperation agreements with several major AI powers. These international relationships provide channels for technical assistance, for influencing the development of international AI standards, and for ensuring interoperability between India's domestic

AI governance framework and the emerging international framework which is essential for India's AI-driven services exports and for Indian AI companies seeking to access global markets.

The path forward for India is therefore a path of principled ambition: ambitious in seeking to build a governance framework that is genuinely protective of fundamental rights and reflects India's constitutional values, but principled in acknowledging the particular developmental context of India and the need to ensure that AI governance serves the larger goal of using AI as a force for inclusive social and economic development. The recommendations of this dissertation centred on an AI Governance Act, amendments to the DPDP Act, reforms to IP law, criminal law, and evidence law, and the establishment of an independent AI Regulatory Authority represent a comprehensive but proportionate response to this challenge.

CHAPTER VIII

CONCLUSION

This dissertation has conducted a systematic study of the legal issues that Artificial Intelligence presents in India, which covers the areas of liability, intellectual property, data protection and privacy, cybercrime, and regulation of the criminal justice system. The discussion has shown that the current legal framework in India, which was developed in the pre-digital era and last modified to address the internet age at best, is fundamentally unprepared to regulate the creation, implementation, and implications of AI systems which are already changing Indian society in both consequential and at times harmful ways.

The paper has found the following key results. First, concerning liability and accountability, the tort law framework of India although theoretically applicable to AI-induced harm under the principles of negligence, strict liability, and the absolute liability principle set in M.C. Mehta v. Union of India has severe limitations in practice in the AI context. The lack of transparency in AI systems, the complexity of determining causation and failure to satisfy the standard of care, and the division of responsibility between the AI value chain impose a responsibility gap that is insufficiently addressed by current laws. The Consumer Protection Act 2019 offers a partial foundation for AI product liability, but it needs extensive interpretation and modification to reflect the risks unique to AI. India is in dire need of an explicit AI liability framework that would explicitly distribute responsibility between developers, deployers, and operators of AI systems.

Second, concerning intellectual property, the Copyright Act 1957 and Patents Act 1970 of India leave the essential questions of AI authorship and inventorship unresolved. The courts are yet to comprehensively decide on whether works created by AI are subject to copyright protection, who owns the copyright, and how the "person who causes the work to be created" criterion of computer-generated works is applicable to sophisticated generative AI systems. It remains unanswered as to whether AI systems are inventors under the Patents Act, and the crucial practical question of whether AI-generated inventions may be patented is unresolved. These questions left unanswered pose serious

legal ambiguity that hinders both the safeguarding of IP rights in AI products and the evolution of an equitable system to compensate human effort in AI research and development.

Third, regarding data protection and privacy, the DPDP Act 2023 is a major legislative achievement, but the law is not as effective as it should be to serve as a sufficient AI governance approach in a number of key aspects. The most severe gaps include the lack of a right to explanation regarding automated decisions, the absence of explicit limitations on AI-driven profiling and discrimination, insufficient terms concerning AI facial recognition technology, and the generous exceptions that can erode the data protection requirements of AI systems used as a part of government functions. The constitutional right to privacy expressed in Puttaswamy is a valuable baseline, yet constitutional principles alone cannot replace specific legislative enforcement.

Fourth, regarding cybercrime and the criminal justice system, the discussion shows not only the ineffectiveness of the current criminal law paradigm in India to combat AI-enabled crimes especially deepfakes, AI-generated CSAM, and AI-powered cybercrime but also the lack of proper legal protections against the threatening potential of AI-based criminal justice tools. The application of AI in situations where fundamental rights of liberty and equality, and rights to fair trials, are directly at risk requires the strictest transparency, accountability, and human oversight requirements.

Fifth, the regulatory environment of India is characterised by fragmentation, sector-focus, and is largely aspirational without the institutional structure, legal power, and technical capacity to regulate the fast-changing AI ecosystem successfully. The lack of a detailed, horizontal AI governance framework risk-based classification, obligatory requirements for high-risk uses, a right to account, a special regulatory body, and effective enforcement is the most fundamental deficiency in the AI governance domain of India.

As a reaction to these results, the dissertation has suggested a detailed set of recommendations based on: the introduction of an AI Governance Act; changes to the DPDP Act to accommodate AI-focused data protection issues; changes to the Copyright and Patents Acts to accommodate AI authorship and inventorship; criminal legislative reforms to accommodate AI-enabled crimes; the creation of an AI Regulatory Authority; and the funding of AI safety research and public education. These suggestions are based on the constitutional principles of India and on the best practices of other countries in the

field, especially the EU AI Act, and are adjusted to the Indian developmental environment and the need to find the right balance between innovation and the protection of fundamental rights.

The creation of an AI governance system that is responsible, rights-protective, and innovation-friendly is not only a technical legal construct, but concerns the future of the type of society that India will become in the next few decades. AI systems have already been deciding about what citizens of India receive credit, who receives a job, who is monitored, who is profiled, and who is a criminal suspect in consequential ways. Without proper legal regulation, such decisions will mirror and reinforce existing inequalities, infringe privacy and dignity, and erode the rule of law. Under proper governance, AI can realise its gigantic potential in the service of human prosperity, hastening the fulfilment of the constitutional guarantee of equality, liberty, and dignity of all Indians.

It is imperative to develop this governance framework. AI is becoming more and more rapid, and the timeframe between proactive regulation and reactive regulation once there is serious harm that is embedded in a person's life grows ever shorter. The legislators, regulators, and courts in India must take action by drawing on the best international experience in formulating strategies that are suitable to the unique constitutional setup of India, its growth goals, and its social context. This dissertation is steered towards that urgent and critical project.

BIBLIOGRAPHY

A. Books

1. Agrawal, Ajay, Joshua Gans and Avi Goldfarb, Prediction Machines: The Simple Economics of Artificial Intelligence (Harvard Business Review Press, Boston, 2018).

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

3. Crawford, Kate, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence (Yale University Press, New Haven, 2021).

4. Duggal, Pavan, Cyberlaw: The Indian Perspective (2nd edn, Saakshar Law Publications, New Delhi, 2014).

5. Eubanks, Virginia, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (St Martin's Press, New York, 2018).

6. Kamath, Nandan, Law Relating to Computers, Internet and E-Commerce (5th edn, Universal Law Publishing, New Delhi, 2018).

7. Marcus, Gary and Ernest Davis, Rebooting AI: Building Artificial Intelligence We Can Trust (Pantheon, New York, 2019).

8. Mitchell, Tom M., Machine Learning (McGraw-Hill, New York, 1997).

9. Pasquale, Frank, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press, Cambridge, 2015).

10. Russell, Stuart and Peter Norvig, Artificial Intelligence: A Modern Approach (4th edn, Pearson, New Jersey, 2020).

11. Walsh, Toby, It's Alive!: Artificial Intelligence from the Logic Piano to Killer Robots (La Trobe University Press, Melbourne, 2017).

B. Journal Articles

1. Abbott, Ryan, 'I Think, Therefore I Invent: Creative Computers and the Future of Patent Law' (2016) 57 Boston College Law Review 1079.

2. Balkin, Jack, 'The Three Laws of Robotics in the Age of Big Data' (2017) 78 Ohio State Law Journal 1217.

3. Buolamwini, Joy and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77.

4. Calo, Ryan, 'Robotics and the Lessons of Cyberlaw' (2015) 103 California Law Review 513.

5. Chesney, Robert and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753.

6. Floridi, Luciano and others, 'An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28 Minds and Machines 689.

7. Hildebrandt, Mireille and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73 Modern Law Review 428.

8. Mishra, Pankaj, 'Algorithmic Justice: Rethinking Criminal Law in the Age of AI' (2023) 45 Journal of Law and Technology 23.

9. Popescu, Andrei, 'The Liability of Autonomous AI: A Comparative Analysis' (2022) 18 Journal of Comparative Law 112.

10. Sparrow, Robert, 'Killer Robots' (2007) 24 Journal of Applied Philosophy 62.

11. Turing, Alan, 'Computing Machinery and Intelligence' (1950) 59 Mind 433.

C. Government Reports and Policy Documents

1. Group of Twenty, G20 New Delhi Leaders' Declaration (G20 2023).

2. Ministry of Electronics and Information Technology, India's Trillion Dollar Digital Opportunity (Government of India, New Delhi, 2019).

3. Ministry of Electronics and Information Technology, Report of the Expert Committee on AI Governance (Government of India, 2023).

4. Ministry of Electronics and Information Technology, Report of the Committee on Non-Personal Data Governance Framework (Government of India, 2020).

5. National Health Authority, Digital Health Blueprint (Government of India, 2019).

6. NITI Aayog, National Strategy for Artificial Intelligence: #AIForAll (Government of India, New Delhi, 2018).

7. NITI Aayog, Responsible AI for All: Adoption Strategy for AI by the Government (Government of India, New Delhi, 2021).

8. NITI Aayog, Cloud & AI Infrastructure Policy (Government of India, New Delhi, 2023).

9. Organisation for Economic Co-operation and Development, OECD Principles on Artificial Intelligence (OECD, 2019).

10. Reserve Bank of India, Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps (RBI, 2021).

11. Srikrishna Committee Report, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, 2018).

12. UK Government, A Pro-Innovation Approach to AI Regulation (Department for Science, Innovation and Technology, 2023).

13. UNESCO, Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021).

14. World Intellectual Property Organization, WIPO Conversation on Intellectual Property and Artificial Intelligence: Third Session (WIPO, 2020).

D. Statutes and Regulations

1. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (Act 18 of 2016).

2. Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023).

3. Constitution of India 1949.

4. Consumer Protection Act 2019 (Act 35 of 2019).

5. Copyright Act 1957 (Act 14 of 1957).

6. Copyright (Amendment) Act 1994 (Act 38 of 1994).

7. Digital Personal Data Protection Act 2023 (Act 22 of 2023).

8. Indian Evidence Act 1872 (Act 1 of 1872).

9. Indian Penal Code 1860 (Act 45 of 1860).

10. Information Technology Act 2000 (Act 21 of 2000).

11. Motor Vehicles Act 1988 (Act 59 of 1988).

12. Patents Act 1970 (Act 39 of 1970).

13. Protection of Children from Sexual Offences Act 2012 (Act 32 of 2012).

14. Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence [2024] OJ L (EU AI Act).

15. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) [2016] OJ L 119/1.

WEBLIOGRAPHY

1. Cyberspace Administration of China, Interim Measures for the Management of Generative Artificial Intelligence Services (2023) <https://www.cac.gov.cn> accessed 18 April 2025.

2. Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed Reg 75191 (30 October 2023) <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence> accessed 18 April 2025.

3. Internet Freedom Foundation, Facial Recognition Technology: Its Uses, Risks and Recommended Reforms <https://internetfreedom.in/facial-recognition-technology/> accessed 18 April 2025.

4. John McCarthy, Marvin L. Minsky, Nathaniel Rochester and Claude E. Shannon, A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence (Dartmouth College, 1955) <http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html> accessed 18 April 2025.

5. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) <https://gdpr-info.eu> accessed 18 April 2025.

6. Regulation (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (Artificial Intelligence Act), OJ L, 2024/1689 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689> accessed 18 April 2025.

7. Securities and Exchange Board of India, Circular on Artificial Intelligence and Machine Learning Application by Market Intermediaries <https://www.sebi.gov.in> accessed 18 April 2025.

8. US Copyright Office, Copyright and Artificial Intelligence: Part 1 – Digital Replicas (US Copyright Office 2023) <https://copyright.gov/ai/ai_policy_guidance.pdf> accessed 18 April 2025.

9. UK AI Safety Institute, The International Scientific Report on the Safety of Advanced AI (Department for Science, Innovation and Technology 2024) <https://www.gov.uk/government/publications/international-scientific-report-on-the-safety-of-advanced-ai> accessed 18 April 2025.