



CELL *for* LAW & TECHNOLOGY

JOURNAL OF LAW AND TECHNOLOGY

VOLUME II

National Law Institute University, Bhopal

NLIU JOURNAL OF LAW AND TECHNOLOGY

VOLUME II

APRIL, 2026

NATIONAL LAW INSTITUTE UNIVERSITY, BHOPAL

Kerwa Dam Road, Bhopal, India – 462 044 (Madhya Pradesh)

The NLIU Journal of Law and Technology is published by the Cell for Law and Technology (CLT) at National Law Institute University, Bhopal.

The NLIU Journal of Law and Technology invites unsolicited manuscripts for publications. Such manuscripts should be submitted in MS Word (.docx format) to clt.editorial@nliu.ac.in. All citations and text conform to *Oscola (4th edn.)*.

All rights reserved. No article or part thereof published herein may be reproduced without the prior permission of the CLT. For all matters concerning rights and permissions, please contact us at clt@nliu.ac.in.

The views expressed in the articles published in this Volume of NLIU Journal of Law and Technology are those of the authors and in no way do they reflect the opinion of the NLIU Journal of Law and Technology, its editors or National Law Institute University, Bhopal.

Mode of Citation:

(2026) 2(1) NLIU JLT

Published by:

The Registrar,
National Law Institute
University, Bhopal
(M.P.) 462044 India

FOREWORD

~ Justice Shyam C. Chandak *

The relationship between law and technology is increasingly shifting from a reactive to an anticipatory one. As digital systems become more embedded in everyday life, the law is required not only to regulate outcomes but also to engage with emerging technological realities from the outset.

Volume II of the *Journal of Law and Technology* reflects this shift through its engagement with pressing contemporary issues. What stands out in this edition is not merely the range of topics but the manner in which they have been approached. The examination of simulated gambling, for instance, captures a regulatory grey area that is rapidly expanding. The blurring of lines between gaming and gambling, particularly through the use of design mechanisms that incentivise continued engagement, raises questions that existing legal frameworks are not yet fully equipped to answer. One is left to consider how, in the coming years, the law might move beyond rigid classifications and instead engage more closely with the underlying effects of such platforms on users.

Similarly, the contributions on artificial intelligence reflect both the immediacy and the complexity of the challenges ahead. The discussion on AI personhood is not merely speculative; it prompts a reconsideration of how legal systems attribute responsibility and recognise agency. At the same time, the analysis dealing with AI in healthcare and accessibility foregrounds more immediate concerns: how liability is to be fixed when decision-making is partly automated, and how technological advancement must remain aligned with principles of inclusion and equity.

The paper engaging with the data protection framework under the Digital Personal Data Protection Act, 2023, is particularly timely. As data-driven models become integral to financial and digital ecosystems, the tension between innovation and fiduciary responsibility becomes more pronounced. The attempt to reconcile data-blind technological architectures with statutory obligations reflects the kind of nuanced inquiry that will be increasingly necessary in this space.

Equally noteworthy is the work on digital currencies, which situates regulatory questions within a broader context of economic sovereignty and resilience. As jurisdictions continue to experiment with different models of regulating digital assets, the role of law in maintaining both flexibility and stability will be critical.

* Justice Shyam C. Chandak is a judge at the Bombay High Court.

The discussion on copyright valuation offers a shift in perspective by bringing together legal and economic considerations. In a digital environment where the value of creative works is both amplified and difficult to quantify, such interdisciplinary approaches are particularly relevant for legal practice. The inclusion of more specialised work, such as that on orbital injunctions, further reflects the expanding horizon of legal questions, many of which extend beyond conventional territorial frameworks.

Taken together, the contributions in this volume reflect a recognition that the law cannot afford to remain static in the face of technological change. At the same time, they also indicate that the answer does not lie in over-regulation, but in developing frameworks that are responsive, context-sensitive, and grounded in fundamental legal principles. Courts and policymakers will increasingly be called upon to adopt approaches that are both technologically informed and jurisprudentially sound.

This journal is a commendable effort in that direction. It demonstrates both intellectual curiosity and a willingness to engage with difficult questions, qualities that are essential for the development of meaningful legal scholarship. I extend my best wishes to the editorial team and the contributors for this publication.

PATRON-IN-CHIEF

Hon'ble Shri Justice Sanjeev Sachdeva

Chief Justice, High Court of Madhya Pradesh, India

PATRON

Prof. (Dr.) S Surya Prakash

Vice Chancellor

National Law Institute University, Bhopal

FACULTY ADVISOR

Prof. (Dr.) Atul Kumar Pandey

Professor

National Law Institute University, Bhopal

PEER REVIEW PANEL**AVNI AIRAN**

Senior Associate, Aapti Institute

CHITRANSH BHANSALI

Associate, AZB

DR. PRASHANT MALI

Advocate

HUSSAIN

Associate, Saraf & Partners

KURUVILA JACOB

Senior Associate, Trilegal

NIKHIL NAREN

Assistant Professor, JGLS

RASHI SHARMA

Associate, Shardul Amarchand Mangaldas & Co.

RITIKA BANSAL

Associate, Shardul Amarchand Mangaldas & Co.

SALONI AGARWAL

Associate, Cyril Amarchand Mangaldas

SANYAM GUPTA

Advocate

SHIVANSH VISHWAKARMA

Associate, Cyril Amarchand Mangaldas

STUDENT BODY OF THE JOURNAL

HANSIKA KUMARI AND SAMRUDHI MEMANE

Editors-in Chief

ALI ASGHAR

Managing Editor

RAJ RAJESHWARI

Executive Editor

Senior Editors

Arpit Dadhich

Divyansh Vyas

Dhruv Pratap Singh

Hiya Saxena

Hemangini Bhati

Ipsa Mittal

Kartika Barsainyan

Rujuta Bapat

Vasudev Mishra

Vibhuti Sharma

Vismaya Tulsian

Yash Singh

Junior Editors

Archit Yadav

Ananya Bhardwaj

Aastha Sharma

Bhumika Alawa

Gannavarpu Rajlakshmi

Mohi Savita

Mohit Rajoriya

Prerna Parmar

Soumil

Sunidhi Pandey

Shivani Tamrakar

Subha Swaminathan

Serena Naidu

Utkarsh Anand

Vikram Singh Rathore

Vaishnavi Tomar

Yashasvi Bhalse

Yashika Chouksey

CONTENTS

EDITORIAL NOTE	7
QUANTIFYING CREATIVITY: APPROACHING COPYRIGHT VALUATION IN THE 21ST CENTURY.....	1
<i>Durgesh Pratap</i>	
IS IT GAMING OR GAMBLING?: EXAMINING THE LEGAL STATUS OF SIMULATED GAMBLING IN INDIA.....	22
<i>Parth Sharma</i>	
RECONCILING THE DATA-BLIND ARCHITECTURE OF ACCOUNT AGGREGATORS WITH SIGNIFICANT DATA FIDUCIARY OBLIGATIONS UNDER DPDP ACT, 2023.....	49
<i>Shivansh Singh and Devdeep Ahirwal</i>	
ALTERNATE APPROACHES TO AI PERSONHOOD: ACCOMMODATING A NEW JURISPRUDENTIAL CHALLENGE.....	63
<i>Prerana Shrinath</i>	
DIGITAL SOVEREIGNTY AND MACROECONOMIC RESILIENCE: ANALYSING INDIA'S REGULATORY FRAMEWORK FOR DIGITAL CURRENCIES.....	76
<i>Bhagyashree Tiwari</i>	
ARTIFICIAL INTELLIGENCE AND DISABILITY RIGHTS: ENSURING EQUITY IN ACCESS AND DESIGN.....	90
<i>Aryan Raj & Shraddha Yadav</i>	
LIABILITY AND ACCOUNTABILITY IN AI-DRIVEN HEALTHCARE: NAVIGATING ETHICAL AND LEGAL CHALLENGES IN MEDICAL MISHAPS..	104
<i>Kavya Pradeep and Jayanth Siva</i>	
ORBITAL INJUNCTIONS: LEGAL REMEDIES FOR SATELLITE-BASED DIGITAL BLOCKADES.....	115
<i>Bhavya Rai</i>	

EDITORIAL NOTE

It is with immense pleasure that we present **Volume II of the Journal for Law and Technology**, marking the continued growth of a publication that began its journey only last year with the release of its inaugural volume. In a short span of time, the Journal has emerged as a significant academic initiative and stands today as a significant academic initiative of the Cell for Law and Technology.

What began as a focused effort to create a platform for discourse at the intersection of law and technology has steadily evolved into a platform that reflects emerging legal challenges in a rapidly digitalising world. Volume II carries forward this vision, building upon the foundation laid by its first edition while expanding both the scope and depth of engagement with contemporary issues.

While this Edition is not confined to a single thematic focus, it reflects a conscious editorial effort to engage with a wide spectrum of concerns ranging from artificial intelligence and digital governance to data protection, financial technologies, and emerging questions of liability and regulation. The contributions collectively demonstrate the dynamic nature of technology law and the necessity of interdisciplinary and forward-looking scholarship.

As technological transformation continues to reshape legal systems, institutions, and societal norms, this Volume seeks to contribute meaningfully to that evolving discourse. It reaffirms the Journal's commitment to fostering rigorous, relevant, and impactful scholarship, while strengthening its identity as a flagship academic endeavour of the Cell for Law and Technology.

The first article, *"Quantifying Creativity: Approaching Copyright Valuation in the 21st Century"*, examines the complexities of valuing copyright in a digital economy by analysing traditional and modern valuation methods. It argues for a hybrid approach combining economic models with legal due diligence, emphasising that risk, originality, and technological change must inform valuation frameworks for greater accuracy.

The second article, *"Is It Gaming or Gambling?: Examining the Legal Status of Simulated Gambling in India"*, analyses India's evolving regulatory framework for online gaming, especially under the 2025 legislation. It highlights ambiguities in defining "online money games" and argues that simulated gambling mechanics blur the line between gaming and gambling, necessitating clearer legal standards.

The third article, *"Reconciling the Data-Blind Architecture of Account Aggregators with Significant Data Fiduciary Obligations under DPDP Act, 2023"*, explores tensions between privacy-centric financial data systems and statutory obligations under the DPDP Act. It argues that the current framework struggles to balance minimal data access with heightened fiduciary accountability.

The fourth article, “*Alternate Approaches to AI Personhood: Accommodating a New Jurisprudential Challenge*”, evaluates the jurisprudential potential of extending legal personhood to AI by drawing an analogy with Indian environmental law cases in which courts have granted personhood to rivers, glaciers, and natural entities.

The fifth article, “*Digital Sovereignty and Macroeconomic Resilience: Analysing India’s Regulatory Framework for Digital Currencies*”, examines India’s approach to regulating digital currencies in light of economic stability and sovereignty concerns. It concludes that regulatory design must balance innovation with financial control and systemic risk management.

The sixth article, “*Artificial Intelligence and Disability Rights: Ensuring Equity in Access and Design*”, discusses how AI systems can both empower and marginalise persons with disabilities. It advocates for inclusive design principles and rights-based regulatory safeguards to ensure equitable technological access.

The seventh article, “*Liability and Accountability in AI-Driven Healthcare: Navigating Ethical and Legal Challenges in Medical Mishaps*”, analyses liability gaps arising from AI-assisted medical decision-making. It argues for clearer attribution of responsibility among developers, healthcare providers, and institutions.

The volume concludes with the eighth article, “*Orbital Injunctions: Legal Remedies for Satellite-Based Digital Blockades*”, which explores emerging legal challenges posed by satellite-controlled digital disruptions. It proposes novel injunctive remedies within both international and domestic legal frameworks to effectively address issues of jurisdiction and enforcement.

This Edition would not have been possible without the unwavering guidance and support of our Faculty Advisor, Prof. (Dr.) Atul Kumar Pandey. His institutional insight and constant encouragement throughout the preparation of this Volume have been invaluable. The Journal owes much of its growth to his mentorship, and we remain deeply grateful for his faith in the editorial process and in the student editors who carry it forward.

We also extend our sincere gratitude to the members of the Editorial and Managerial Board, whose tireless efforts, often behind the scenes, ensured the timely and rigorous completion of this Volume. Their commitment to editorial excellence, attention to detail, and engagement with complex submissions form the backbone of the Journal. We are equally thankful to our peer reviewers for their careful evaluations and constructive feedback, and to our authors for entrusting the Journal for Law and Technology with their work. Scholarly publishing is inherently collaborative, and this Volume stands as a reflection of that shared commitment.

As the Journal for Law and Technology moves forward from its first edition, this Volume is not merely a continuation but a reaffirmation of purpose. The Journal remains committed to fostering substantive and forward-looking scholarship, and to providing a platform for voices engaging with the evolving interface of law and technology. It is in this spirit that we present Volume II.

Hansika Kumari and Samrudhi Memane

Editor-in-Chief and Deputy Editor-in-Chief

QUANTIFYING CREATIVITY: APPROACHING COPYRIGHT VALUATION IN THE 21ST CENTURY

— Durgesh Pratap*

ABSTRACT

Valuation is an inseparable aspect of intellectual property management that enables rights holders to monetize their creations effectively. With the advent of new forms of IPs and rapid technological advances, from cutting edge software, video games, media franchises, streaming services to more traditional forms of copyright and invaluable works of art, comparing and evaluating the effectiveness of valuation methods becomes a vital necessity in the 21st century. Although traditionally considered to be the exclusive domain of economists and accountants, IP valuation today requires integrating legal due diligence with economic frameworks. Therefore, this study explores copyright valuation by bridging accounting mathematics with legal risk assessment. To this end, it explores various methodologies used to assess the economic value of copyright, including traditional approaches such as the cost method, market method, and income method, including asset approach, MEEM method, direct cash flow method, discounted cash flow method and relief from royalty method. The paper also discusses alternative models, such as the auction method, 25% rule, pay-off method, and fuzzy evaluation technique, providing additional insights into quantitative valuation. Additionally, the study identifies key legal, creative, market and technological risks which introduce unpredictability into purely traditional quantitative economic models. The paper contributes by assessing the relevance and redundancy of these valuation methods with respect to concurrent state of technology while also suggesting the 5Ws & H approach as a qualitative-quantitative hybrid tool for selecting an appropriate valuation method. Through this exercise, by emphasising the importance of a multi-faceted and hybrid approach for accurate valuation, the study adds to the evolving discourse of copyright valuation to keep up with the demands of practical utility in evolving copyright ecosystems.

Keywords: *Intellectual Property Valuation, Copyright Valuation, Valuation Methods, Comparison of Valuation Methods, Role of Risk in Copyright Valuation.*

* Durgesh Pratap is a student of LL.M. (IPR) at National Law University, Jodhpur.

I. INTRODUCTION

Intellectual property rights are a category of intangible assets which can be owned by individuals, firms, etc. Economists view IPR as a means to drive innovation and derive adequate returns from such creative activities.¹ Intellectual property law gives exclusivity to the owner of the intellectual property (IP) to exploit the rights related to that IP for a limited period of time.² These rights can also be transferred in the form of licenses or assignments. This allows a creator to transfer the rights associated with an IP to another party. These rights are also subject to protection by law when there is infringement.

The balance sheet of a business shows all of its assets, liabilities and capital. Among its assets, both *tangible* and *intangible* assets are covered. It is easier to determine the value of *tangible assets* like property, equipment, machinery etc. However, it is rather difficult to assign a value to *intangible assets* because their value depends on the expectation of earnings.³ Therefore, intellectual property assets need to be valued in order to effectively exploit them. Various factors may serve as IP valuation triggers. These might be, for example, corporate valuation for shareholders, IPO, regulatory compliances, financial reporting, assignment or licensing of an IP asset, investment or further research and development in the IP asset, corporate mergers and acquisitions, fundraising etc.⁴

Copyright by its nature is fundamentally the exclusive right to give others the right to do, or stop others from doing, certain things with specific kinds of works protected under the Copyright Act.⁵ An economic value can be attached to copyright which would then facilitate the owner of the copyright to enter licensing or other commercial arrangements with another party in exchange for royalty or some other financial advantage.⁶ Copyright is a bundle of rights which allow or restrict the conduct of other persons in relation to a work in various ways and can be exploited financially. For example, in the case of cinematographic films there are various ways to exploit such a copyright. This can be in the form of theatrical release, music videos, soundtracks, sequels, television screenings, theme parks, restaurants, merchandise, etc. As such, a cinematograph film's proprietor may grant licences to distributors and broadcasters

¹ Christine Greenhalgh and Mark Rogers, 'The Value of Intellectual Property Rights to Firms and Society' (2007) 23(4) Oxford Review of Economic Policy 541, 542.

² Akshat Pande, *Valuation of Intellectual Property Assets* (Eastern Law House 2010) 26.

³ Lloyd Austin, 'Accounting for Intangible Assets' (2007) 9(1) University of Auckland Business Review 63.

⁴ Paul Flignor and David Orozco, *Intangible Asset & Intellectual Property Valuation: A Multidisciplinary Perspective* (World Intellectual Property Organization 2006) 2–3.

⁵ Alka Chawla, *Law of Copyright: Comparative Perspectives* (LexisNexis 2013) 7–8.

⁶ World Intellectual Property Organization, *Valuing Intellectual Property Assets* (WIPO Business & Finance, undated) <<https://www.wipo.int/en/web/business/ip-valuation>> accessed 9 April 2026.

for the purpose of theatrical releases, disc rentals, geographical broadcast and releases, satellite broadcast, etc.⁷ Thus in order to make the most of such copyright, it is necessary to determine the value of such an asset.

IP valuation is treated more as the domain of accountants and economists than of legal professionals. Consequently, IP valuation and copyright valuation remain confined to purely quantitative considerations. This may result in overlooking underlying legal nuances while copyright gets treated as merely a cash flow generating mechanism. This paper seeks to bridge the gap between accounting mathematics and legal due diligence, by arguing for a hybrid quantitative and qualitative approach with copyright valuation. For this purpose, doctrinal and analytical methodologies have been employed to critically examine traditional and alternative valuation frameworks along with the variables emerging from risks associated with IP.

The Section II of this paper expands into quantitative methods of the copyright valuation with various traditional and alternative techniques. Among them, income method has been discussed in more detail than the rest, owing to its diverse sub approaches with unique applications, for the purpose of advancing the discourse on copyright valuation. Section III delves into the qualitative risks that are associated with copyright valuation. Section IV deals with how and what method to employ while valuing copyright works along with identifying the factors needed to be considered for copyright valuation. The final section of the paper concludes with its findings laid out along with making practical suggestions for valuing copyright works in the 21st century.

II. COPYRIGHT VALUATION METHODS

For an IP asset to be valued, it is required that a company:⁸

- (1) Performs identification of its IP assets.
- (2) *Assign* a justifiable value to the IP assets that are identified.

An IP audit would help in the evaluation and identification of all of the company's assets including intellectual properties.⁹ However, valuation requires a more nuanced approach.

⁷ Vanessa Van Coppenhagen, 'The Valuation of Copyright' (2004) 16 South African Mercantile Law Journal 353, 354.

⁸ Jody C Bishop, 'The Challenge of Valuing Intellectual Property Assets' (2003) 1 Northwestern Journal of Technology and Intellectual Property 59, 60.

⁹ G Gouri and K Jain, 'Intellectual Property Audit for Efficient Intellectual Property Management of an Organisation' in 2012 Proceedings of PICMET'12: Technology Management for Emerging Technologies (IEEE 2012) 894, 895.

Valuing copyright works is similar to valuing real estate. For example, in residential real estate, a property may be valued by looking at similar transactions but where a property is unique and there are no equivalent examples in the market, it is difficult to assess the value of that property.¹⁰ Hence, different methods need to be employed.

A host of approaches can be employed for the purpose of valuation of copyright works. These are discussed as follows.

A. Cost Approach

The cost approach method of valuation is used to quantify the future economic benefit of an IP in today's time.¹¹ This is done by evaluating the cost of replacement or reproduction of the said IP while also factoring in the obsolescence.¹² Therefore, it contemplates the cost of developing an alternate IP which would produce similar benefits. Cost, however, does not adequately indicate value as something may require high input costs yet is unable to deliver adequate economic benefits. This method helps in obtaining either the cost of reproduction i.e., creating a replica or the cost of replacement i.e., creation of an IP with identical utility.¹³

This method requires the factoring of historical costs which need to be converted into trended costs by translating them in today's time. Historical cost includes the cost incurred in advertising, investment, production, litigation cost, legal fee, registration fees etc.¹⁴ An IP may also become redundant overtime as a result of obsolescence. This obsolescence may come in the form of functional, technological, or economic obsolescence. These factors also need to be considered while determining the value of an IP using the cost approach. The following formula can be utilized to arrive at a fair market value for an IP.

$$FMV_{IP} = C_r - O$$

where,

FMV_{IP} = Fair market value of IP

C_r = Cost of replacement/reproduction

O = Obsolescence

¹⁰ Russell L Parr, *Intellectual Property: Valuation, Exploitation, and Infringement Damages* (5th edn, 2018) 91.

¹¹ Bishop (n 8) 64.

¹² Parr (n 10) 93.

¹³ Gary Speier and Raj Gupta, 'Intellectual Property Valuation: Asset Strength Approach (Evaluation of the Strength of an Asset Against the Commercial Technology Covered by the Asset)' (SSRN, 20 May 2015) 4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615115> accessed 9 April 2026.

¹⁴ Alina Saaranto and Ahti Salo, 'A Review of the Methods for Valuing Intellectual Property Rights' (Independent Research Project, Aalto University, 29 September 2016) 6. <https://sal.aalto.fi/publications/pdf-files/esaa16_public.pdf> accessed 9 April 2026.

The cost approach with respect to copyright would be employed to assess the cost incurred in the creation of music, songs, films or other artistic works.¹⁵ However, with respect to copyright works, such sort of information is not easily accessible, which makes it difficult to use the cost approach for the purpose of valuation. The nature of copyright works is unique and a fair comparison is often not possible. It also needs to be noted that as a bundle of rights that can be separately licenced and exploited in different slices, copyright by its nature is similar to an economic pie and the cost approach does not fully capture this nature.¹⁶ For example the creation of *Chacha Chaudhary* comics by Pran cannot be accurately valued by the cost method as it would only consider the cost of the paper, ink and the amount of hours put in by the creator. However, the amount of creativity put in by the creator would go unaccounted for. Scholars rightfully assert that cost does not equate to value.¹⁷ As such, the cost method would not prove to be effective in this case.

B. Market Approach

The market approach looks at comparable transactions of similar IPs in a market to arrive at a fair value. It is based on the principle that market forces of demand and supply determine a fair and justified price for a particular property.¹⁸ However, it is necessary that such a transaction must take place in a public market place and it should be an arm's length transaction of similar properties.¹⁹ It is also necessary to account for the motivation of buyers, market conditions as well as various distorting factors.²⁰

There are further challenges associated with this approach, namely, finding comparable IPs or adequate public information about licensing. Private transactions and trade secrets limit the amount of information that is available in the public domain. The market approach can still be applied if there is no data available regarding comparable IP transactions but there is data available regarding the business entity as a whole in which the intellectual property resides.²¹ Subtracting the value of all other assets and the value of business enterprise, the residual value

¹⁵ Anis Mashdurohatun, Andri Winjaya Laksana and HM Ali Mansyur, 'Valuation Method of Intellectual Property Rights for Copyright Products of Small and Medium Enterprises as Objects of Credit Guarantees Benefit-Based in the Digital Era' (2023) 9 <https://doi.org/10.2991/978-2-38476-022-0_9> accessed 9 April 2026.

¹⁶ Van Copenhagen (n 7) 358.

¹⁷ Parr (n 10) 84.

¹⁸ Saaranto and Salo (n 14) 7.

¹⁹ WIPO Asian Regional Forum on the Intellectual Property Strategy for the Promotion of Innovative and Inventive Activities, *Valuation of Intellectual Property Assets; Valuation Techniques: Parameters, Methodologies and Limitations* (Taejon, Republic of Korea, 22–24 November 2000) WIPO/INN/DDK/00/5(a) 3.

²⁰ Harald Wirtz, 'Valuation of Intellectual Property: A Review of Approaches and Methods' (2012) 7(9) *International Journal of Business and Management* 40, 42.

²¹ Van Copenhagen (n 7) 359.

would result in the value of *intangible assets* which would also include the IP assets.²² However, this technique would assume that the market is perfectly informed about the business enterprise's intellectual property asset's value. This is a major flaw of this method.²³ Another major challenge associated with this method is that copyright works are unique in nature, and therefore, it is hard to perform a fair comparison between different copyright works. For example, *Pokémon* is considered to be the highest revenue generating IP in the world.²⁴ Using the market approach to value the IP as a whole would prove to be very difficult because of the uniqueness of the IP and the lack of comparative IPs which could be used as a yard stick to determine its value. Hence, the market approach would not be appropriate in this case.

C. Income Method

The income approach primarily emphasizes upon the income producing capability of the IP asset.²⁵ It contemplates upon the future income streams that would be generated by the IP asset. Therefore, the value of the IP asset is determined by calculating the present worth of the net economic gains it is expected to generate throughout its useful life.²⁶ Scholars have agreed that there are three parameters which are paramount to the income method.²⁷ They are as follows:

1. The future income stream
2. The duration of the income stream
3. The risk associated with the realisation of income stream

The American sitcom TV show *FRIENDS* which started airing in early 90s still enjoys a large viewership despite the show ending its run on television two decades ago.²⁸ Its rights are still highly sought after by streaming services as its income generation capacity is significant. The income method finds itself appropriate for assessing the value of such an IP.

Various sub approaches can be identified based on the above parameters. These sub approaches have been highlighted further.

i. The Asset Approach

The asset approach or the residual technique is a method of intellectual property valuation where the entire value of the business is taken as a whole including all of the assets which make

²² *ibid.*

²³ *ibid.*

²⁴ Brent Koepp, 'Pokémon Has Become the Highest Grossing Media Franchise of All Time' (*Vice*, 31 July 2025) <<https://www.vice.com/en/article/pokemon-has-become-the-highest-grossing-media-franchise-of-all-time>> accessed 9 April 2026.

²⁵ *Bishop* (n 8) 64.

²⁶ *ibid.*

²⁷ *Wirtz* (n 20).

²⁸ *The Economist*, 'Why "Friends" Is Still the World's Favourite Sitcom, 25 Years On' (*Prospero*, 20 September 2019) <<https://www.economist.com/prospero/2019/09/20/why-friends-is-still-the-worlds-favourite-sitcom-25-years-on>> accessed 9 April 2026.

up the business enterprise.²⁹ Thereafter the value of all tangible and intangible assets is determined, which leaves behind the value of IP assets as residue. For example, *Disney* completed its acquisition of *21st Century Fox* for a total of USD 71 billion.³⁰ This value is attributed to the entirety of *Fox's* assets. If one were to apply the asset approach to determine the value of the IP assets held by *Fox*, the value of the workforce and executive team, studio equipment, customer contracts and licensing deals, streaming technology, and other tangible and intangible assets, would have to be determined separately to isolate the value of the company's various IP assets.

This approach has been criticized on grounds that it is an indirect method of valuation and primarily depends upon the valuation of the entire business enterprise and its tangible and intangible assets excluding intellectual property assets. This leaves margin for error and requires a great degree of precision.³¹ It is also argued that it is impossible to isolate the residual value from the rest of the assets and business enterprise given the nature of interdependence and interplay between various assets, departments and components of a business enterprise. Mere mathematical residual calculations cannot be relied upon in light of these criticisms.

ii. Direct Cash Flow Method

The DCF method or earning methodology stipulates that income generated from the IP asset can be readily identified. Once such income flow is generated, it can be easily identified and valued.³² For example, where an intellectual property is licenced and hence generates revenue from that said licence, the value of that intellectual property can be reliably quantified for the near future. This method is only possible where the IP asset is generating income. Where there is no income, this method cannot be used.³³ *Codex Leicester*, a scientific manuscript written by Leonardo da Vinci in the early 1500s is an example of how splendidly this method fails when there is no income stream associated with it. The *Codex Leicester* is like a dormant gold mine sitting in Bill Gates' private collection, not actively earning money, but clearly is immensely valuable.³⁴ Its potential lies in history, prestige, and future uses, not in on-going income.

²⁹ *Van Coppenhagen* (n 7) 361

³⁰ Junya Li, 'Analysis of the Walt Disney's Acquisition of 21st Century Fox' (2023) *Highlights in Business, Economics and Management* 14, 40, 41 <<https://doi.org/10.54097/hbem.v14i.8960>> accessed 9 April 2026.

³¹ *Van Coppenhagen* (n 7) 361.

³² *Wirtz* (n 20) 43.

³³ *Van Coppenhagen* (n 7) 361.

³⁴ Anna Blume, 'Codex Indulgence: Leonardo's Codex Leicester and the Issue of Value' (1997) 2(2) *On Paper* 16.

iii. Relief from Royalty Method

The idea behind relief from royalty method is that by owning an IP in its entirety, a proprietor needs not to pay for licensing fees or any other form of royalties in order to exploit his intellectual property.³⁵ Where a property or asset owned by the proprietor could be useful eternally, this method would calculate the cash flow for perpetuity.³⁶ Of course, this only applies theoretically in the case of copyright as copyrighted works enter the public domain once their statutory term of protection expires. Still, while employing the relief from royalty method within the period where the copyrighted work is protected, the discounted cash flow model is adopted as the amount of economic benefit derived from the asset is only for a finite time period.

$$\frac{\text{Royalty Saved}}{\text{Capitalization Rate}} = \text{Value}$$

Here, the royalty saved is the amount saved by the proprietor due to owning intellectual property and capitalization rate is the rate of return that the owner earns. The value hence obtained is the calculated value of intellectual property.

Take for example the case of the *Unreal Engine* used in game development. As one of the leading game engines in the gaming industry, various developers and studios have to license it from its creators and owners of Epic Games.³⁷ However, since Epic Games also makes its own games and owns *Unreal Engine*, it doesn't have to pay any licensing fees and is therefore exempted from paying any royalties. Hence, the relief from royalty method finds its applicability here.

The relief from royalty method only represents the income stream from a portion of the economic benefit from the asset being valued. It does not take into picture the entire value of the asset and merely accounts for the royalty and licensing fees.³⁸ The method also requires similar IP assets in order to determine the value of the asset at hand. Due to the unique nature of copyright works, finding similar assets is not viable and hence, comparable assets need to be looked at to determine a prevailing royalty rate in the market.

³⁵ Robert Reilly, 'Relief from Royalty Method of Intellectual Property Valuations' (2022) LVII(1) *Les Nouvelles: Journal of the Licensing Executives Society* 19 <<https://ssrn.com/abstract=4019626>> 9 April 2026.

³⁶ *ibid.*

³⁷ Matt Craig, 'Epic Games' Unreal Money Engine' (*Forbes*, 10 November 2023) <<https://www.forbes.com/sites/mattcraig/2023/11/10/epic-games-unreal-engine-fortnite-game-developers-sypherpk/>> accessed 9 April 2026.

³⁸ *Parr* (n 10) 102.

iv. Discounted Cash Flow Method

The discounted cash flow method works by assessing the value of the asset by discounting the projected future cash flows. It is used to calculate the present value of an asset by discounting its future cash flows back into its present value.³⁹ In a DCF analysis, the economic income derived from the asset is projected for several time periods in the future. Afterwards, the projected income is then converted into present value by discounting it using present day rates. The risks are also taken into account while determining the cash flows.⁴⁰ For example, high risk cash flow such as video games would need to be discounted more heavily than the cash flows of a product that is less risky, say a novel or another literary work. The former is more volatile compared to the latter. The DCF method may prove useful for valuation of a copyright work due to it being a more precise analysis and being more easily verifiable. To further understand this concept, an IP like *Harry Potter* can be referenced. The franchise has spawned multiple books, plays, games, movies, even theme parks, with a television series on the way.⁴¹ The books, even after years of release, still enjoy a large readership whereas the video games lose relevance within a few years of their release. Hence, under the DCF method the games would be discounted more heavily than the books.

v. Multi-Period Excess Earnings Method

MEEM values the IP asset by determining the portion of income generated by the asset after subtracting relevant costs of contributory assets used in producing that income. The excess earning is then discounted to its present value using a risk-adjusted discount rate.⁴² To employ MEEM, the future cash flows need to be evaluated from the area of business, which includes the IP asset. This could pose a challenge if the cash flows produced by the IP are not separately indicated in the company's balance sheet. The contributory asset charges also have to be taken into consideration. These may be labour, machinery, land, capital or other rights, etc. Afterwards, the present economic value of future cash flows needs to be discounted and converted while also accounting for the time and risk. For the purpose of determining risk, the cost of capital is used according to the circumstances of the object to be valued.⁴³ In most cases the *weighted average cost of capital* is used as cost of capital.

$$WACC = CE \cdot \frac{VE}{VD} + CD \cdot (1 - R) \cdot \frac{VD}{VC}$$

³⁹ Wirtz (n 20) 42.

⁴⁰ *ibid.*

⁴¹ Alys Davies, 'Harry Potter Books to Be Made into New TV Series' (*BBC News*, 12 April 2023) <<https://www.bbc.com/news/entertainment-arts-65258807>> accessed 9 April 2026.

⁴² Saaranto and Salo (n 14) 11.

⁴³ Wirtz (n 20) 43.

Where,

WACC = weighted average capital cost

CE = cost of equity

CD = cost of debt

R = rate of tax

VE = market value of equity

VD = market value of debt

VC = market value of total capital

Using this WACC helps calculate the present value for the said IP asset. Discount factor is calculated through the formula mentioned below. This is finally used to calculate the present value.⁴⁴

$$D = \frac{1}{1 - WACC}$$

$$PV = \sum_{t=1}^{t=n} CF_t \cdot D$$

Where,

D = discount factor

PV = present value

n = useful life of the IP asset

CF_t = cash flow in period t

The MEEM is suitable for use where IP economic benefits are difficult to identify directly. It provides a theoretical method for determining the cash flow of individual assets that make up the total income stream.

D. Auction Method

The auction method is particularly useful for copyright works. It finds its origin in the public auctions of musical works in London between the 19th and 20th century. Engraved plates of musical works were auctioned to the general public and the price determined by these auctions gave an idea about the price of similar works available in the market.⁴⁵ The copyright to the songs was also sold along with the plates, which is why the name *copyright auctions* came to

⁴⁴ Saaranto and Salo (n 14) 11.

⁴⁵ Ruth Towse, 'Copyright Auctions and the Asset Value of a Copyright Work' (2016) 13 Review of Economic Research on Copyright Issues 83, 83.

be. The catalogue of many auction houses listed the information of the buyer and seller as well as the title and the composer of the works being sold. These served as an important source of determining the value of similar musical works. Such auctions and catalogues also served as a source of information regarding price swings for a particular work. For example, *The Last Milestone* fetched £225 (£25,787) in 1891 and then in 1905 the same musical work sold for £531 (£58,239).⁴⁶ The change in prices and trends indicated the change in demand and sentimentalities of the people and therefore, served as indicators of changing market trends and values for musical works.

E. The 25% Rule Method

The 25% rule is a methodology devised by Robert Goldscheider to determine a reasonable royalty rate for the purpose of licensing IP assets. The method is also called the rule of thumb method.⁴⁷ The licensee retains 75% of the profit due to the substantial development, commercialization, risk, investment and other resources put into the asset by him while the 25% is retained by the licensor. The rule serves as an important starting point of negotiations for licensing and royalty transactions.⁴⁸ Focus is made on long run agreements due to the inherent nature of IP assets' capacity to generate income over a long time. Although primarily used for patents, the method has seen use in trademark and copyright royalty and licensing negotiations as well.

The rule has found support from the courts as well. In *Standard Manufacturing Co., Inc. and DBP, Ltd. v United States*,⁴⁹ The court found that the 25% rule was an appropriate method for the purpose of evaluating the baseline royalty rate. The rule has, however, been subjected to criticism that it is a crude tool and has been seen as arbitrary.⁵⁰ It is also argued that the 25% rule varies depending upon the type of industry the intellectual property asset finds its use upon, given that the rates may go as high as 30 or 40%.⁵¹ Still, as reiterated above, it primarily serves as a yardstick for starting negotiations.

F. Pay-Off Method

The pay-off technique is an analysis technique designed for valuing assets, especially those with uncertain and difficult to estimate future cash flows. The basis of the pay-off approach is

⁴⁶ *ibid* 93–94.

⁴⁷ Robert Goldscheider, 'The Classic 25% Rule and the Art of Intellectual Property Licensing' (2011) 10 Duke Law & Technology Review 1, 1.

⁴⁸ *Parr* (n 10) 247.

⁴⁹ *Standard Manufacturing Co Inc and DBP Ltd v United States* 42 Fed Cir 748 (1999 US Claims LEXIS 11).

⁵⁰ Robert Goldscheider, John Jarosz and Carla Mulhern, 'Use of the 25 Per Cent Rule in Valuing IP' (2002) 37(4) *les Nouvelles* 123, 130.

⁵¹ *ibid*.

in its three value scenarios which are: (1) *Best guess scenario* which denotes the most likely estimated value, (2) *Optimistic scenario* which points towards the maximum possible value and; (3) *Pessimistic scenario* which relies on the minimum possible value.⁵² Afterwards a pay-off distribution is created which facilitates the calculation of a mean value.

For example, *The Witcher* franchise, though originally limited to just a series of novels, the IP has expanded into a multimillion franchise spawning a Netflix adaptation with multiple seasons and various games which have sold exceptionally well.⁵³ To apply the pay-off method, one would have to calculate the best guess scenario, optimistic scenario, and pessimistic scenario. The best scenario would anticipate steady game sales are achieved, Netflix renews its license, and a solid merchandise base is established. The pessimistic scenario would expect that game sales dwindle and the series dies out. Optimistic scenario, would hope the game sequels hit big, Netflix spin-offs succeed, new film deals are made. With these three numbers, a pay-off distribution would be created and then the resulting possible mean value would serve as the IP's value.

The method provides a comparison of assets over time within a portfolio which helps proprietors and investors make better decisions. The approach has also been found useful by various corporations in intellectual property management. This approach also provides for *real options thinking* under which copyrights may gain value over time due to market trends, new distribution channels or adaptations of works via real option value calculation.⁵⁴

G. Fuzzy Evaluation Method

The fuzzy evaluation method can also be employed for the purpose of valuation of copyright works. This model has been used by scholars to value online movies in China.⁵⁵ In a study, the researchers took three of the most popular Chinese movie distribution platforms namely *iQIYI*, *Tencent* and *Youku*. An index was also created using the Delphi method by compiling answers from a questionnaire presented to a large number of experts. The index contained various parameters such as the theme of the movie, the influence of the director, writer, producer, actor

⁵² Mikael Collan and Markku Heikkilä, 'Enhancing Patent Valuation with the Pay-off Method' (2011) 16 *Journal of Intellectual Property Rights* 377, 379.

⁵³ Antonio Pequeño IV, 'Witcher 3 Video Game Sells Over 50 Million Copies, Company Says—Nearing These Other Top-Selling Games' *Forbes* (29 May 2023) <<https://www.forbes.com/sites/antoniopequenoiv/2023/05/29/witcher-3-video-game-sells-over-50-million-copies-company-says-nearing-these-other-top-selling-games/>> accessed 9 April 2026.

⁵⁴ Collan and Heikkilä (n 52) 379–80.

⁵⁵ P Song, Y Liu and J Sun, 'Research on the Copyright Value Evaluation Model of Online Movies Based on the Fuzzy Evaluation Method and Analytic Hierarchy Process' (2023) 11 *Systems* 405 <<https://doi.org/10.3390/systems11080405>> accessed 9 April 2026.

etc., themes, pre-release and post-release reception, running time, popularity online, online review platform ranking, entertainment etc.

Using python software and the fuzzy evaluation method as well as the analytic hierarchy process, weightage was assigned to each movie based on the aforementioned index.⁵⁶ The following formulae were used in determining value of online movies;

$$X_{ij} = \sqrt[n]{\prod_{k=1}^n X_{ij} \cdot X_{kj} \cdot i}, j \in N$$

$$M_i = \prod_{i=1}^n X_{ij} (i=1,2,...,n)$$

$$W_{nm} = W_n \cdot C_{nm}$$

where,

X = complete consistency matrix

M_i = product of factors of each row of judgement matrix

W_{nm} = composite weight of second level index

This model of valuation is unique and innovative as it provides an avenue in the valuation of emerging copyright works such as online movies. However, this model can be criticized on the basis that due to the nature of the index prepared in the study, it is not widely recognised or accepted anywhere else. If this method were to be applied to *Bollywood* movies, an index would have to be generated from scratch. Going through the above mentioned steps would give an index to evaluate the movies. The index thus prepared would also be bound by the same limitation, i.e. it would not be applicable anywhere else. The method also fails to capture the very dynamic nature of the online movie market and industry and hence, does not foresee upcoming changes and challenges. The method's self-contained design is perhaps both its strength and its primary weakness.

III. THE ROLE OF RISK IN COPYRIGHT VALUATION

Although valuation of copyright works naturally would be derived from applying the aforementioned methodologies, valuation does not occur in isolation. There needs to be a quantitative assessment of various other risks in order to obtain successful valuation of an IP asset. Various such risks are discussed in this section of the study.

⁵⁶ *ibid.*

A. Legal Risk and Enforcement

If a copyright work has questionable legal basis, it is difficult to provide valuation for such an asset. It is thus necessary to determine if such a work is really valid. Even though it is not required to register copyright works, registering them serves as proof of authorship and ownership.⁵⁷ A person also needs to act upon their copyright or else their silence to act would be considered as estoppel and acquiescence.⁵⁸ The Indian Supreme Court has upheld the principle of acquiescence in recent judgements as well, stating that acquiescence unlike limitation eliminates the right itself.⁵⁹ Therefore, it is important to consider whether the work which is subject to valuation is protected under the necessary laws or whether the proprietor has acquiesced to the infringement of his work. Additionally, the remaining term of a copyrighted work directly impacts its inherent value. The Indian Copyright Act explicitly states the term of copyright for different types of works.⁶⁰ The closer the work is to the expiry of its term of protection, the lower its value will be. In terms of valuation, this would mean that upon using *income method*, the legal risk would need to be appropriately accounted for and in both the cases; it would bring down the aggregate value of the copyrighted work.

B. Technological Risk

In the case of software, there is the risk of obsolescence as with each passing day, new and better software enters the market. This reduces the lifetime and usability of the software at hand and makes it particularly vulnerable to the advancements in the industry.⁶¹ Similar to how despite launching with much fanfare and huge investment from Microsoft, *Windows Phone* was driven out of the market and rendered obsolete by *iOS* and *Android*.⁶² Since *income methods* such as DCF (discounted cash flow) and MEEM are based on calculating future income streams, a technology becoming obsolete would significantly hinder the income generating capacity of the IP. Hence, these methods would yield the best results to accurately calculate the value of the work as these sufficiently contemplate upon risk posed by technological obsolescence.

⁵⁷ Robert J Kasunic, 'The Benefits of Registration' (2020) 68 J Copyright Soc'y USA 83, 84.

⁵⁸ *Policansky Bros v Hermann and Canard* 1910 TPD 1265.

⁵⁹ Prachi Bhardwaj, "'Acquiescence virtually destroys the right of the person": SC distinguishes acquiescence from delay and laches' (*SCC Online Blog*, 19 November 2021) <<https://www.sconline.com/blog/post/2021/11/19/acquiescence-virtually-destroys-the-right-of-the-person-sc-distinguishes-acquiescence-from-delay-and-laches/>> accessed 9 April 2026.

⁶⁰ The Copyright Act, 1957 (14 of 1957) ss 22-29.

⁶¹ Peter Sandborn, 'Software Obsolescence—Complicating the Part and Technology Obsolescence Management Problem' (2007) 30(4) IEEE Transactions on Components and Packaging Technologies 886–888.

⁶² Ewan Spence, 'Windows Phone Is Dead, Long Live Microsoft's Smartphone Dream' (*Forbes*, 12 July 2017) <<https://www.forbes.com/sites/ewanspence/2017/07/12/microsoft-windows-phone-windows10-mobile-strategy/>> accessed 9 April 2026.

C. Market Risks

Demand is one of the primary drivers of the market and also determines the value of a copyright work. As such, the popularity of the work directly influences the income streams that can be derived from it and its exploitation. In industries such as music and cinematography films, successful advertisement and promotion also play a huge role in driving up the demand for such work.⁶³ The works which are more recognizable and accepted over a large geographical area or internationally enjoy high value. The nature of the market i.e., the relevant market as well as barriers to entry must also be taken into account while determining the value of a copyright work. For instance, today there is a large demand all over the globe for queer romance literature and dramas, with China in recent years emerging as a major market player.⁶⁴ But recent government crackdowns on such works have severely impacted both the output⁶⁵ and consumption⁶⁶ of such media in the nation. Countries such as Thailand have consequently emerged to fill the vacuum,⁶⁷ but it is hard to say whether the same crackdown as China would not take place there as well. Therefore, such kind of market risks also need to be taken into account.

Competition, piracy and emerging technology also pose risk to the works at hand. Emerging technologies and rising competition can drastically change the market landscape, as in the case of today's AI driven software market. Tech giants like Wipro, Infosys and Oracle have seen not only layoffs,⁶⁸ but have also suffered fall in share prices as well as fall in demand of their software and other services due to the rise of AI.⁶⁹ Accounting for these market risks while determining the value of the software and products of these companies would be a crucial component while employing income methods of valuation.

⁶³ Dongling Huang, Andrei Strijnev and Brian Ratchford, 'Role of Advertising and Consumer Interest in the Motion Picture Industry' (2015) 13(1) *Review of Marketing Science* 1.

⁶⁴ Yiming Wang, 'Pure Love and Shadow Desire: Navigating Censorship, Queer Fantasy and Ressentiment in Chinese Boys' Love (BL) Erotica' (2026) *European Journal of Cultural Studies* 13675494261421517, 2.

⁶⁵ Shahana Yasmin, 'Mounting public anger in China as writers of gay erotic fiction face prosecution: "Unreasonable and ignorant"' *The Independent* (1 July 2025) <<https://www.independent.co.uk/asia/china/gay-erotica-china-danmei-writers-arrested-b2779488.html>> accessed 9 April 2026.

⁶⁶ Hannah Ellis-Petersen, 'China bans depictions of gay people on television' *The Guardian* (4 March 2016) <<https://www.theguardian.com/tv-and-radio/2016/mar/04/china-bans-gay-people-television-clampdown-xi-jinping-censorship>> accessed 9 April 2026.

⁶⁷ Amporn Jirattikorn, 'Chinese Fandom of Thai Boys' Love Dramas: Shipping the Queer Romance and Fan Service Practices' (2025) *Global Media and China* 20594364251385213, 2.

⁶⁸ Jon Markman, 'Oracle's Massive 30,000 Layoff As AI Spending Surges' *Forbes* (6 April 2026) <<https://www.forbes.com/sites/jonmarkman/2026/04/06/oracles-massive-30000-layoff-as-ai-spending-surges/>> accessed 9 April 2026.

⁶⁹ Amit Mudgill, 'Anthropic AI tool: Why Infosys, TCS, Wipro, HCL fell up to 6% today' *Business Today* (4 February 2026) <<https://www.businesstoday.in/markets/stocks/story/anthropic-ai-tool-why-infosys-tcs-wipro-hcl-fell-up-to-6-today-514504-2026-02-04>> accessed 9 April 2026.

D. Degree of Originality

The degree of originality of a copyright work also has a direct impact on the risk associated with the income stream. Although copyright works by their nature are original,⁷⁰ works with higher creative originality enjoy greater protection and are potentially more valuable. For example, the remake *O Sajna* of the classic song *Maine Payal Hai Chhankai* from 1999, could not garner the same level of interest as the original. The original has 460 million views on the singer's Vevo channel while the remake garnered 55 million views on the T-Series channel on the same platform *Youtube*. It was subjected to harsh criticism on the internet as well.⁷¹ Therefore, creative originality plays a crucial role in the commercial success of a copyright work.

IV. HOW AND WHAT METHOD TO PICK?

Having discussed the methods of valuation in detail and their usage and the different risks involved in copyright valuation, the question of what valuation method to pick in a given situation naturally arises. From the viewpoint of mathematics, obtaining an answer to a problem is a matter of merely inputting the value of variables in a mathematical equation. Similarly, the various approaches when employed would each theoretically provide an estimate value for the copyright work. However, it is up to the valuation professional to determine the best possible method(s) to obtain an accurate valuation.

This can be easily understood by the example of *Grok's* valuation, xAI's generative artificial intelligence model.⁷² If the *cost method* were to be employed to value *Grok*, that would only account for the development cost of creating it. The *cost approach* does not adequately serve the purpose of accurately valuing *Grok*. If the *market approach* is adopted to determine *Grok's* value, comparison would have to be drawn to similar AI models in the market such as *ChatGPT*, *Claude*, *Gemini*, etc. Although multi-billion dollar valuations of OpenAI⁷³ and

⁷⁰ The Indian Copyright Act, 1957 (14 of 1957) s 13(1).

⁷¹ Akshat Sundrani, 'Neha Kakkar Slammed for Recreating Iconic Song "Maine Payal Hai Chhankai", Netizens Say "Maaf Karo Hume"' (*India TV News*, 23 September 2022) <<https://www.indiatvnews.com/entertainment/music/neha-kakkar-slammed-for-recreating-90s-song-maine-payal-hai-chhankai-netizens-troll-2022-09-23-810785>> accessed 9 April 2026.

⁷² x.ai, 'Grok' (x.ai) <<https://x.ai/grok>> accessed 9 April 2026.

⁷³ Antonio Pequeño IV, 'OpenAI Valuation Reaches \$852 Billion After Massive Funding Round' *Forbes* (31 March 2026) <<https://www.forbes.com/sites/antoniopequenoi/2026/03/31/openai-valuation-reaches-852-billion-after-massive-funding-round/>> accessed 9 April 2026.

Anthropic⁷⁴ have been seen, the valuation of their specific models have not been isolated, which makes using *market approach* difficult.

The *income method* would be the best method among the traditional three methods of valuation, since the future income streams, their duration and the associated risks could be reliably determined. Even among *income method*, some approaches are better suited for valuing *Grok* than others. xAI was reportedly valued at 250 billion USD in its merger with SpaceX.⁷⁵ If one were to apply the *asset approach*, all of xAI's intangible and tangible assets aside from *Grok* would have to be determined. The residual value would give us the valuation of *Grok*. Since doing so would prove to be very difficult, the *asset approach* would not be an ideal method for this purpose. Moving to *relief from royalty method*, it could be argued that since X (formerly twitter) uses *Grok*, the platform saves on licencing fees that would have otherwise went in the integration of another generative AI. Although Microsoft and Apple have both made deals to integrate *ChatGPT* into their systems, the integration of X and *Grok* is qualitatively and vertically unique in nature and hence, makes it difficult to determine a prevailing royalty rate. In *DCF* (discounted cash flow) and *MEEM* approach, *Grok's* future cash flows would have to be discounted appropriately while factoring in risks. In this aspect, there could be various kinds of risks that would affect valuation. For example, the price of computer components in building data centres, availability of electricity, the possibility of *Grok* falling behind its peer LLM models, and market shifts such as the bursting of the 'AI bubble' constitute some of the major risks that would increase the discount rate. Legal and regulatory hurdles also constitute significant risk as nations may contemplate banning *Grok*.⁷⁶

Among alternative valuation methods, the *auction method* would be unsuitable for valuing *Grok* as *auction method* for copyright works is now mostly obsolete. The *25% rule* could be used to negotiate a licencing deal for *Grok*, but a negotiation can go either side. It could go below 25% or above it as the 25% rule is not an iron rule. With the *pay-off method*, three scenarios would have to be contemplated for *Grok*. For argument's sake, these three scenarios could be: (1) an *optimistic scenario* where *Grok* keeps gaining new subscriptions, stays technologically ahead of other LLM models and dominates the market share. (2) a *pessimistic*

⁷⁴ 'Anthropic Valued at \$380 Billion in Latest Funding Round' *Reuters* (12 February 2026) <<https://www.reuters.com/technology/anthropic-valued-380-billion-latest-funding-round-2026-02-12/>> accessed 9 April 2026.

⁷⁵ Nick Robins-Early, 'Elon Musk announces merger of SpaceX and xAI' *The Guardian* (3 February 2026) <<https://www.theguardian.com/science/2026/feb/02/elon-musk-spacex-xai-merger>> accessed 9 April 2026.

⁷⁶ Foo Yun Chee, 'EU lawmakers support ban on AI apps generating explicit images' *Reuters* (18 March 2026) <<https://www.reuters.com/legal/litigation/eu-lawmakers-support-ban-ai-apps-generating-explicit-images-2026-03-18/>> accessed 9 April 2026.

scenario where *Grok* lags behind other models and sees its user base dwindle. (3) a *best guess scenario* where *Grok* shows steady growth and remains competitive. Creating a pay-off distribution of the three scenarios would facilitate the calculation of a mean value. Although the *fuzzy evaluation method* could be used for valuation of LLM models after creating an index of different performance parameters with the help of industry experts, the method is better suited for works such as movies or literature where there is a large number of comparable works available.

Though all the methods would provide some value for *Grok*, it is questionable if the method chosen would be appropriate. For the *Grok* case mentioned, considering all the factors, DCF or MEEM seem to be the most appropriate and accurate valuation methods. It must be noted that there is no iron rule that only one single method must be employed for valuation. A combination of approaches could be utilized to gain a more accurate valuation of the asset by arriving at a median value. It would serve to provide an accurate valuation while reducing the error margin to a minimum.

To obtain an accurate valuation of copyright works, the valuation professional would have to consider all the factors causing the variation of value and their significance to choose the most appropriate method for that particular copyright work. Consequently, the *5Ws & H* technique based on *who*, *where*, *when*, *what*, *why* and *how* questions can serve as inspiration to evaluate the problem at hand from various directions.⁷⁷ This would be done by identifying the various factors that are required in choosing a specific valuation method. A simple checklist of these factors could serve as a good starting point. First, the valuator must determine *who* owns the copyright to the work and if there is a need to secure licensing or account for other stakeholders. Subsequently, there must be determination of *what* the nature and originality of the work are, alongside the cost of creating or replacing it. It should also be considered *where* the work stands in the present market, specifically looking for comparable market transactions that are accessible for analysis. Furthermore, it is essential to establish *when* the term of copyright expires while assessing its overall useful life along with the duration of its projected income streams. The valuator must also understand *why* the valuation might fluctuate by identifying various inherent risks and determining if the work is at risk of becoming obsolete. Finally, they must determine *how* the work generates income, i.e. whether those cash flows are predictable, and how the copyright work could be separated from other tangible and intangible assets.

⁷⁷ Vesna Čančer, 'Criteria weighting by using the 5Ws & H technique' (2012) 3(2) Business Systems Research 41, 47.

Taking all of these factors into account would greatly facilitate the decision making process on which method or combination of methods to choose from during valuation.

V. CONCLUSION AND THE WAY FORWARD

The valuation of copyright works is imperative to maximising the economic potential of creative assets. Through proper evaluation, right holders can more effectively monetize their work via licensing royalties and other commercial avenues. Valuation also proves to be essential in reflecting intangible assets in the financial statements of businesses. It is also found that for activities such as, mergers acquisitions, investments, and regulatory compliance, the process of valuation is indispensable.

Upon analysing the various methods of valuing intellectual property assets, it can be concluded that some techniques are more suitable for the purpose of copyright valuation than others depending on the specific copyright work. While each valuation method has its strengths and limitations, a combination of approaches often yields the most accurate results.

For easy visualisation, the findings have been presented in tabulated form. The table gives a brief description of strengths and weaknesses for the methods examined in this paper. A recommended value is suggested to denote the usability of each method in the digital age.

Table 1: Key Characteristics of Various Copyright Valuation Methods in the Digital Era

Valuation Method	Remarks	Recommended Value*
Cost Approach	gives value of reproducing similar work, ignores creativity of copyright	weak/specific use
Market Approach	gives reference value for copyright, ignores uniqueness of copyright	neutral/specific use
Income Approach	focused on income generation capacity of the IP	strong
Asset Approach	depends on residual value method, leaves error margin	weak/not recommended

Valuation Method	Remarks	Recommended Value*
Direct Cash Flow	uses generated income to evaluate, unusable when no income generated	neutral/specific use
Relief From Royalty	calculates future income streams via prevailing royalty rates	neutral/specific use
Discounted Cash Flow/MEEM	determines present value of future cash flows by discounting	strong
Auction Method	popular during 19th century	obsolete
25% Rule	useful for starting negotiations, inadequate for direct use	neutral/specific use
Pay-off Method	used when future cash flows are difficult to estimate	neutral
Fuzzy Evaluation Method	creates index to qualitatively assess works, requires wide acknowledgement of index	strong/specific use

**The Recommended Value refers to the degree to which a certain method is recommended for, 'Strong' value denotes a high recommendation value, while 'neutral' and 'weak' denote to medium and low respectively. Additionally, 'specific use' denotes to methods that are useful in particular situations on a case by case basis.*

In the discussion above, it has become adequately clear that valuation cannot occur in a vacuum, i.e. various other factors must be considered for fruitful results. There is more to copyright valuation than quantitative mathematics, given that copyright itself is an intricate and intangible bundle of rights. The thorough understanding of the legal provisions and intricacies of copyright that a legal professional possesses is completely different from economists and accountants who view copyright as simply a cash flow generating mechanism. For instance, a DCF (discounted cash flow) or MEEM assisted valuation would fail if it were to overlook risks such as the strength of the title, risk of statutory acquiescence or borderless infringement. Examining such risks from a legal point of view would reduce the unpredictability and

volatility from the economist's calculations. Hence, legal due diligence is vital for successful and precise copyright valuation.

Additionally, examining the various valuation techniques bring into view the limitations of traditional approaches to valuation. Media, entertainment and copyright works for the matter are primarily digitised and technologically driven in the 21st century. Most works today are either at the risk of rapid technological obsolescence, have zero or almost zero marginal cost of reproduction, or are entirely unique in nature. As such, industrial-era techniques such as cost approach appear to lose their relevance. This is especially true when it comes to digital works. Similarly, the unique nature of digital works as well as increasing secrecy in licencing agreements make the market approach increasingly unusable as well, owing to the lack of comparable transactions.

Keeping all of the above in mind, the principal recommendation of this study is that valuation should not remain confined to just quantitative calculations but must transition into a hybrid model that is both qualitative and quantitative. To achieve this outcome, it is recommended that the 5Ws & H framework be adopted. By determining the *what*, *who*, *where*, *when*, *why* and *how* of a digital asset, a valuation professional could ensure a valuation that is both qualitative and quantitative. The most effective valuation strategy for 21st century where digital works continue to evolve would be a legally informed multi-disciplinary approach.

IS IT GAMING OR GAMBLING?: EXAMINING THE LEGAL STATUS OF SIMULATED GAMBLING IN INDIA

—Parth Sharma*

ABSTRACT

Recently, the centre notified The Promotion and Regulation of Online Gaming Act 2025 and has invited comments on the draft rules framed under the same. The act provides for regulation of online games through an Online Gaming Authority, which marks a departure from the self-regulatory model under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021. In this regard, this paper first examines the procedural aspect involved in regulation of online games in India by comparing the effectiveness of regulation by the state, vis-à-vis self-regulation. The 2025 act also places a blanket prohibition on those games categorized as an “online money game” but fails to provide adequate clarity on the scope of the definition of the same. This then leaves game developers and authorities in a limbo when designing games and enforcing the act and its rules respectively. This is a problem because the growth of the online gaming industry in India in the past two decades has led to the emergence of a vast variety of online games, with many adopting multiple gameplay models simultaneously. Such games, through a variety of mechanisms, incorporate a ‘random chance’ element to their games to encourage users to spend more time playing such games. Therefore, the second part of the paper examines the structural similarities between such simulated gambling and real-world gambling. It further examines whether, in light of the rapidly evolving nature of online gaming, the legal definition of online gambling, requires a revisit.

Keywords: *Simulated Gambling, Online Gaming Regulation, Online Money Game, Gaming Addiction, Random Reward Mechanisms, Real Money Gaming, India.*

* The author is a legal researcher at the Rajasthan High Court.

I. INTRODUCTION

Online gaming in India is a rapidly expanding sector which is growing at a Compound Annual Growth Rate of 10% between 2023 and 2026 to cross a size of INR 388 billion by 2026.¹ This is in tandem with the growing online presence in India, with approximately 1 billion internet users (as on December 2025)² (a considerable increase from a little over 259 million, as on June 2014)³ and with an internet penetration of 61.62% (as per a 2023 reply in parliament).⁴ A considerable factor behind this growth lies in the affordable access to internet, with the average cost of 1GB data being reported in 2025 as INR 9,⁵ with a per capita income in the same year being USD 2820.⁶ This rise in internet penetration and online presence of Indians can be said to be an aiding factor in the rise of online gamers in India, which stood at 42.5 crore in financial year 2023, which is the second highest number globally.⁷ Amongst this large population of online gamers in India, 77% of the gaming revenue from India is generated from “*real money gaming*”, with the average paying user spending USD 20 per annum (in the financial year 2022).⁸

With such a considerable portion of the Indian population playing online games, many of whom are minors, it becomes imperative to ensure that the designs being incorporated in such games are mindful of consumer health and welfare. This issue with regards to the susceptibility of minors to such addiction was also recognised previously and can be described through the observation of a court in *New York*, which opined that “*children often act impulsively or without good judgment*” and hence cannot be said to grant their consent for dangers emerging

¹ Invest India, ‘Gaming Industry in India’ <<https://www.investindia.gov.in/sector/media/gaming>> accessed 1 November 2025.

² Telecom Regulatory Authority of India, ‘The Indian Telecom Services Performance Indicators October-December, 2025’ (*Telecom Regulatory Authority of India*, 3 March 2026) <https://www.trai.gov.in/sites/default/files/2026-03/QPIR_03032026_0.pdf> accessed 8 April 2026.

³ Brijendra Singh and others, *Statistical Year Book 2015* (Ministry Of Statistics And Program Implementation) <https://mospi.gov.in/sites/default/files/Statistical_year_book_india_chapters/INFORMATION_TECHNOLOGY.pdf> accessed 11 January 2026.

⁴ Dr. Ramapati Ram Tripathi and others, ‘Internet Connectivity in Rural Areas’ (Lok Sabha, Session No. 11, 2023) <<https://sansad.in/getFile/loksabhaquestions/annex/1711/AU2351.pdf?source=pqals>> accessed 27 June 2025.

⁵ Subhayan Chakraborty, ‘India will be data capital of the world in 5 years: Jyotiraditya Scindia’ (*Business Standard*, 29 May 2025) <https://www.business-standard.com/industry/news/india-to-become-data-capital-in-5-years-says-jyotiraditya-scindia-125052901766_1.html> accessed 10 January 2026.

⁶ International Monetary Fund, ‘GDP per capita, current prices’ <<https://www.imf.org/external/datamapper/NGDPDPC@WEO/IND/BGD>> accessed 10 January 2026.

⁷ Aviral Godha and others, ‘New Frontiers: Navigating the evolving landscape for online gaming in India’ (*Ernst and Young*, 2023) <<https://www.ey.com/content/dam/ey-unified-site/ey-com/en-in/insights/media-entertainment/documents/ey-new-frontier-online-gaming-report.pdf>> accessed 27 June 2025.

⁸ Ernst and Young, ‘Windows of opportunity: India’s media & entertainment sector-maximizing across segments’ (*Ernst and Young*, 2023) <<https://www.ey.com/content/dam/ey-unified-site/ey-com/en-in/newsroom/2023/5/images/ey-ficci-report.pdf>> accessed 11 January 2026.

consequently and law should not assume otherwise.⁹ Furthermore, in the context of the *United States* (“US”), there have been discussions on introduction of reforms aimed at regulation for addictive technologies, including providing of warnings and establishing codes of conduct, with *Matthew B. Lawrence* arguing that legislation on such technology can be justified under the 13th Amendment, enabling creation of legislation to enforce the prohibition on “*involuntary servitude*”.¹⁰

In India, various members of parliament have time and again raised the issue of the prevalence of gaming addiction in parliament, particularly amongst adolescents.¹¹ In 2022, *Vivek Narayan Shejwalkar*, a member of parliament (“MP”), citing the issue of gaming addiction amongst minors in India, also recommended setting up of a regulatory board for games along the lines of the film censor board in India to evaluate appropriateness of games prior to their launch.

In this regard, the 2023 amendment (“**2023 amendment**”) to the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021* (“**Intermediary Guidelines**”) mandated self-regulatory bodies to take measures to safeguard users against the risk of gaming addiction¹². More recently, *The Promotion and Regulation of Online Gaming Act* (“2025 Act”) was notified, imposing a ban on games which are an “*online money game*” and establishing an Online Gaming Authority for regulation of such games.¹³

In 2018, the *World Health Organization* included “*gaming disorder*” as a “*clinically recognizable and clinically significant syndrome*”,¹⁴ and defined it in the 11th revision of the *International Classification of Diseases*, which describes it as an “*impaired control over gaming*” to the extent that the user begins to prioritize it over other activities in life despite

⁹ *Trupia v Lake George Cent. School Dist.* 14 NY3d 392.

¹⁰ Matthew B. Lawrence, ‘Addiction and Liberty’ (2023) 108(259) *Cornell Law Review*, 295-297 <<https://publications.lawschool.cornell.edu/lawreview/wp-content/uploads/sites/2/2023/04/Lawrence-final.pdf>> accessed 24 May 2025.

¹¹ Vishu Datt Sharma, ‘Abetting Video Games’ (Lok Sabha, Session No. 12, 2023) <<https://sansad.in/getFile/loksabhaquestions/annex/1712/AU3238.pdf?source=pqals>> accessed 29 May 2025; Jaskaur Meena, ‘Online Gaming Activities’ (Lok Sabha, Session No. 15, 2024) <<https://sansad.in/getFile/loksabhaquestions/annex/1715/AU797.pdf?source=pqals>> accessed 29 May 2025; The Online Gaming (Regulation) Bill, 2022, LS Bill (2022-23) (78), Statement of Objects and Reasons; S. Jothimani, ‘Impact of Online Gaming Addiction’ (Lok Sabha, Session No. 4, March 19, 2025) <https://sansad.in/getFile/loksabhaquestions/annex/184/AS262_CTKaSZ.pdf?source=pqals> accessed 1 November 2025.

¹² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) (Amendment) Rules 2023, G.S.R. 275(E), r 6 (IT Rules Amendment).

¹³ The Promotion and Regulation of Online Gaming Act 2025, chs III, IV (Online Gaming Act).

¹⁴ ‘Inclusion of “gaming disorder” in ICD-11’ (*World Health Organization*, 14 September 2018) <<https://www.who.int/news/item/14-09-2018-inclusion-of-gaming-disorder-in-icd-11#:~:text=Gaming%20disorder%2C%20with%20its%20online,their%20pattern%20of%20gaming%20behaviour>> accessed 23 January 2025.

suffering from negative consequences.¹⁵ This classification was also cited by *Vivek Narayan* in 2022, while recommending the need for a regulatory board for gaming. This difference between ‘impaired control’ and ‘knowledge’ will be the topic of the discussion further in the paper.

The legal right against such kinds of addictions can arguably be said to form part of one’s “*freedom of thought*”.¹⁶ In this regard, *Lawrence* argues that addiction interferes with an individual’s autonomy by compelling an individual to have “*unwanted thoughts*”, distracting them from those thoughts which are of their choosing, altering (in severe cases) an individual’s behaviour contrary to how they wish to behave and alteration of an individual’s “*brain structure and chemistry*” to do the first three.¹⁷ Therefore, *Lawrence* defines such “*freedom from addiction*” as the “*freedom from repetitive, intrusive thoughts to engage in harmful behaviours*”.¹⁸

Furthermore, on the subject of addictive game designs and their harm to user health, it would be reasonable to argue for regulation of addictive game designs as other similarly addictive materials are also regulated by the state, like the prohibition on the consumption and sale of narcotic and psychotropic substances under *The Narcotic Drugs and Psychotropic Substances Act 1985*,¹⁹ or the local regulations in India, setting minimum age limits, as well as limiting places for sale of alcohol.²⁰ Though, such assertions of negative effects of online games, as the *Karnataka High Court* opined, must be based not on the traditional models but considered on the touchstone of recent internet modes with the former requiring a reconsideration and appropriate modifications being made basis collection and evaluation of comprehensive data.²¹ This scientific basis of gaming addiction (discussed further in the paper) will form the basis for the arguments framed in the paper.

In this context, the second chapter examines the different regulatory approaches adopted by the centre and in the state of Tamil Nadu, namely that of co-regulation and state regulation respectively for regulation of online gaming. As these regulations will also be addressed in subsequent chapters, this chapter provides the procedural aspect of online gaming regulation prior to discussions on the substantial aspect. The third chapter examines the problems

¹⁵ International Classification of Diseases (11th revision, 2018) <<https://icd.who.int/browse/2025-01/mms/en#1448597234>> accessed 2 January 2026.

¹⁶ *Lawrence* (n 10), 273-275, 305, 309.

¹⁷ *ibid* 283.

¹⁸ *ibid* 309.

¹⁹ The Narcotic Drugs and Psychotropic Substances Act, 1985 ss 2 (viii) (iii) 4 (1).

²⁰ The Delhi Excise Act, 2009 s 23 (Delhi Act); The Delhi Excise Rules 2010, F. 10(8)/Fin(Rev.-1)/2010-11/SSF/104, r 51(1) (Delhi Rules); The Madhya Pradesh Excise Act, 1915, s 23 (MP Act).

²¹ *All India Gaming Federation v The State of Karnataka* 2022 SCC OnLine Kar 435 [XVIII(b)].

associated with defining ‘addictive games’ mainly through the lens of financial harm (including a comparison with the stance in Tamil Nadu), including the concept of “*non-monetary gambling*”. In this regard, it also highlights the challenges arising out of a watertight definition of ‘games of skill’ and ‘games of chance’ in light of the evolving nature of online games. The fourth chapter provides a conclusion to all the above discussions.

II. DIFFERENT REGULATORY APPROACHES FOR ONLINE GAMES IN INDIA

Prior to discussing the specific nuances of the substantive portion of relevant regulations, it is important to understand the underlying structures enforcing the same. In India, there exist different regulatory models for the regulation of online games. Broadly, there exist three approaches to regulation, i.e., self-regulation, co-regulation and state regulation.²² The first approach entails direct regulation by the government, with supporters of this approach arguing it is necessary to protect users from the “*self-interested behaviour*” of companies.²³ The second approach advocates for self-regulation by the market and industry and opposes state intervention on grounds that regulation by the former will deliver better results and that companies already have an incentive of protecting user privacy to avoid “*losing customers*”²⁴ (this can be applied to online gaming as well, in the sense that companies have an incentive to avoid harms like addiction from their games to avoid state intervention).

The third approach encourages undertaking those initiatives for which both the state and industry share responsibility in drafting and enforcing regulations, with supporters arguing that it provides the oversight and rigor of state regulation whilst also maintaining the adaptability provided by self-regulation, enabling such regulation to keep up with needs of the digital realm.²⁵ In this chapter, the co-regulatory and state regulation models provided for under the *Intermediary Guidelines, Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Act 2022* (“TN Gaming Act”) and the 2025 Act respectively would be examined.

²² Dennis D. Hirsch, ‘The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?’ (2011) 34(2) Seattle University Law Review 440-441 <<https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2003&context=sulr>> accessed 30 June 2025.

²³ *ibid* 440.

²⁴ *ibid*.

²⁵ Hirsch (n 24) 441.

A. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

Regulations for online gaming do exist, with the *Ministry of Electronics and Information Technology* (“Meity”) being allotted the said subject in 2022 vide an amendment to the *Allocation of Business Rules 1961*,²⁶ which then amended the Intermediary Guidelines in 2023 to frame regulations for online gaming in India.²⁷ One of the objectives behind introduction of the amendment is combating addiction amongst adult and minor users (particularly financial losses to adults owing to such addiction).²⁸ Furthermore, the Minister of State for Meity had previously said that “*permissible online games*” (monetary or non-monetary) under these rules would be such games which do not lead to children getting addicted.²⁹

Prior to examining the regulatory structure, it is important to examine the debate surrounding the legislative competence of the centre to legislate on the said subject. This becomes important because, in light of the 2023 Amendment, it has been questioned whether such a central rule encroaches on the right of states to legislate on the said subject. This is because, while mediums of communication (including wireless communication) fall within the Union List,³⁰ the subject of gambling and betting, as well as sports and entertainment, fall within the State List.³¹ Some argue this to be a positive move, mentioning that a central rule will ensure parity and uniformity in the applicable law across the country.³²

The *Law Commission of India* had opined that since those kinds of betting and gambling happening online take place over different kinds of media (including telephones, wireless, broadcasting, etc.) which are in turn within the scope of the Union List, therefore, the Parliament has the legislative competence to legislate on the same.³³ However, the commission did add that gambling, being a state subject, can be legislated upon by a state’s legislature

²⁶ The Government of India (Allocation of Business) (Three Hundred and Seventieth Amendment) Rules 2022, S.O. 6062(E), r 2(i) (Allocation of Business Rules Amendment).

²⁷ Ministry of Electronics & IT, ‘Government ushers in new era of responsible online gaming through strict guidelines for ensuring safety of Digital Nagriks and accountability of online gaming industry’ (Press Release No. 1918383, Press Information Bureau, 2023) <<https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=1918383®=3&lang=1>> accessed 3 January 2026.

²⁸ *ibid.*

²⁹ TechDesk, ‘Breaking down MeITY’s new online gaming rules: How it will impact the Indian gaming industry’ (*The Indian Express*, 9 April 2023) <<https://indianexpress.com/article/technology/gaming/meity-new-online-gaming-rules-explained-8544334/>> accessed 26 December 2024.

³⁰ The Constitution of India 1950, sch VII, List I, Item 31 (Constitution).

³¹ The Constitution of India 1950, sch VII, List II, Item 33 and 34 (Constitution).

³² Alaukik Shrivastava and Kashish Siddiqui Khan, ‘Online Gaming Laws in India: An Analysis of the Legislative Intent Vis-À-Vis the Future Roadmap’ (2024) 14(2) UNLV Gaming Law Journal, 163-164 <<https://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1224&context=glj>> accessed 5 October 2025.

³³ Law Commission Of India, *Legal Framework: Gambling And Sports Betting Including In Cricket In India* (Report No. 276, 2018) 116.

(subject to the national gambling policy and “*other legal considerations*”).³⁴ However, there does exist literature countering this view. For example, it has been argued that with increasing digitization, many activities previously carried out offline have shifted online.³⁵ However, such digitization should not mean merely because some activity is now done over the internet, that the same would now fall under the jurisdiction of Parliament, which would have the effect of rendering entries in the State List redundant.³⁶

In this regard, the Supreme Court in *State of Maharashtra vs Bharat Shanti Lal Shah and others*,³⁷ while referring to the ‘doctrine of pith and substance’, the court highlighted the need to delve into the “*true character*” of the concerned enactment (including its objective, scope and effect) to ascertain whether the same falls within legislative scope of a particular legislature as provided under the constitution. In this regard, it was argued that the word “*communication*” under Entry 31 of the Union List be read restrictively so as to leave some room for legislative enactments by state legislatures.³⁸ While the Supreme Court has previously held that the power granted under an entry in the 7th Schedule has to be read to include “*incidental and ancillary*” matters, it also noted that an entry in the Union List which is meant for general regulation of a subject cannot override the regulation of a specific aspect under the State List.³⁹

Also, it would be difficult to justify an interpretation of ‘communication’ encompassing ‘betting and gambling’ as well. As the subjects of gambling and betting (without any distinction or specification made as to the medium over which such activities are carried out) are more specific in nature than wireless (or other form of similar communications). Basis the said judgement, the state legislatures would have the right to legislate on the same.

Coming to the regulatory structure itself, within the amended version of these rules, an entity (subject to certain criteria which shall be discussed further) can seek to be designated as an ‘online gaming self-regulatory body’ by Meity.⁴⁰ These rules do not limit the number of self-regulatory bodies⁴¹, which would then lead to confusion and inconsistency with regards to interpretation and application of certain criteria for verification of a game as a permissible

³⁴ Ibid.

³⁵ Shrutanjaya Bhardwaj, ‘Regulating The Online Gaming Industry: Legislative And Executive Competence, (2023) 5 NLUJ Journal of Legal Studies <<https://lnkd.in/gupCMUbW>> accessed 3 January 2026.

³⁶ Ibid.

³⁷ (2008) 13 SCC 5 [43].

³⁸ Shrutanjaya Bhardwaj (n 38).

³⁹ While in this case, the Supreme Court was examining the levy of tax on betting and gambling under the Union and State Lists and held that power to levy tax cannot be considered to be an “*incidental and ancillary matter*”, the principle enumerated is relevant here as well. See *State of Karnataka v State of Meghalaya* 2022 SCC OnLine SC 350 [151], [159.1].

⁴⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 4A.

⁴¹ *ibid*

online game. To illustrate this point, the rules empower such self-regulatory body to devise a framework which shall also introduce measures to safeguard its users against gaming addiction, including issuance of warning messages (more frequently) for prolonged gaming and an option for the user to self-define their monetary and time limits on gaming.⁴²

The first lacuna is the potential misuse of the scope of interpretation of what would constitute ‘combating gaming addiction’. This is further exemplified by the fact that gaming addiction has not been statutorily defined in India. This would lead to forum shopping, whereby companies producing such online games would seek certification from certain self-regulatory bodies which are likely to provide a more favourable interpretation of the criteria laid down in the rules. In this regard, while speaking on the differing opinions delivered by different constitutional courts, the *Chief Justice of India* recently suggested a “*uniform national judicial policy*” to combat the said issue.⁴³ This suggestion can also be applied in the context of online gaming, including the Online Gaming Authority (as the centre can designate multiple authorities to assist the Online Gaming Authority under the 2025 Act as well).⁴⁴

Furthermore, the provisions allow the user to themselves self-opt for monetary and time limits on gaming for themselves.⁴⁵ This provision is in line with the answer provided by the former Minister of State in Meity in parliament, stating that the government does not intend to impose any such time limit on online games.⁴⁶ This method is also effective because it has been found that a “*risk minimization approach*” (allowing users to make informed choices and encourage responsible gaming behaviour) is more effective than blanket bans.⁴⁷

The second lacuna is that having a self-regulatory body, with membership which is representative of the gaming industry,⁴⁸ to devise frameworks for self-regulations may raise concerns pertaining to conflict of interest. This conflict is particularly true in the context of framing rules to tackle the issue of gaming addiction. As discussed above, 77% of the gaming revenue in India is generated from “*real money gaming*”.⁴⁹ This is coupled with the fact that

⁴² *ibid* r 4A (8) (d).

⁴³ PTI, ‘CJI Surya Kant bats for uniform national judicial policy, says time ripe to reinforce predictability’ *The Economic Times* (26 November 2025) <<https://economictimes.indiatimes.com/news/india/cji-surya-kant-bats-for-uniform-national-judicial-policy-says-time-ripe-to-reinforce-predictability/articleshow/125594110.cms?from=mdr>> accessed 29 November 2025.

⁴⁴ Online Gaming Act, s 8 (1).

⁴⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 4A (8) (d).

⁴⁶ Dr. Niyati Pandey and Tarun, ‘Evaluating Blanket Bans and Mandatory Limits in Gaming’ (Gujarat National Law University, 2024) <<https://gnlu.ac.in/Document/content-docs/1b3b905c-7d50-48c1-b6c0-5dbada252935.pdf>> accessed 17 June 2025.

⁴⁷ *ibid*.

⁴⁸ IT Intermediary Rules, r 4A (2) (b).

⁴⁹ Ernst and Young (n 8).

previously, a positive correlation between spending money on video gaming activities and video game addiction (alongside factors like time spent on such games) has been observed.⁵⁰ This means that the self-regulatory body is entrusted to regulate gaming firm's source of revenue (in the form of time and money spent on games), which is a conflict of interest.

This conflict was also recognized by the government, who rejected multiple proposals for self-regulatory bodies in 2024 as they failed to meet the composition criteria for the board,⁵¹ as well as being too dominated by “*gaming companies and their industry associations*” instead of representing “*a wider base*”.⁵² To combat this, that it was reported in March of 2024, that *National Law University Delhi* in collaboration with the *E-Gaming Federation* was preparing recommendations for Meity for the establishment of an independent online gaming regulator which shall only allow registered entities to offer online games in India.⁵³

B. Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Act 2022
Tamil Nadu in 2023, enacted the TN Gaming Act, to regulate online gaming and gambling. For enforcement of the provisions of the act, it provides for a creation of an online gaming authority by the state government.⁵⁴ However, since the act has been passed with the purpose of regulating the online space, there is debate on the legislative competence of a state legislature to enact a law regulating the digital space (including online gaming and gambling), which is a central subject, with such a view also being adopted by the Meity in 2023⁵⁵ (with online gaming being allotted as a subject to the said ministry in 2022).⁵⁶

The composition of the authority as per the act is a person retired from a rank at least equivalent to the Chief Secretary (as the chairperson), a retired police officer (not below the rank of

⁵⁰ Amir Zaib Abbasi and others, ‘Predicting Video Game Addiction Through the Dimensions of Consumer Video Game Engagement: Quantitative and Cross-sectional Study’ (2021) 9(4) JMIR Serious Games <<https://games.jmir.org/2021/4/e30310/PDF>> accessed 30 November 2024.

⁵¹ Kashish Aggarwal, ‘Govt to regulate the online gaming industry whilst awaiting for proposals to set up SRO by the industry’ *Et Legal World* (28 February 2024) <<https://legal.economictimes.indiatimes.com/news/law-policy/inability-to-reach-a-consensus-on-the-formulation-of-a-sro-might-affect-the-economy-of-the-gaming-industry-says-experts/108067077>> accessed 26 December 2024.

⁵² Jatin Grover, ‘No SRO for online gaming, Govt to act as regulator’ *Financial Express* (12 February 2024) <<https://www.financialexpress.com/business/brandwagon-no-sro-for-online-gaming-govt-to-act-as-regulator-3391156/>> accessed 26 December 2024.

⁵³ Himanshi Lohchab, ‘NLU preparing recommendations for a online gaming regulator, to submit to MeitY soon’ (*The Economic Times*, 25 March 2024) <<https://economictimes.indiatimes.com/tech/technology/govt-plans-independent-regulator-for-online-gaming/articleshow/108754450.cms?from=mdr>> accessed 26 December 2024.

⁵⁴ Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Act 2022, s 3 (TN Online Gaming Act).

⁵⁵ Soumyarendra Barik, ‘How Tamil Nadu and the Centre have locked horns over the issue of online gaming’ *The Indian Express* (12 April 2023) <<https://indianexpress.com/article/explained/explained-law/online-gaming-how-tamil-nadu-and-the-centre-have-locked-horns-over-the-issue-8550409/>> accessed 7 December 2024

⁵⁶ Allocation of Business Rules Amendment, r 2(i).

inspector general) (as member), information technology expert (as member), psychologist (as member), and online gaming expert (as member).⁵⁷ This composition differs from the central rules to the extent that it does not include an educationist, child rights specialist, an individual with experience in promoting online game users interests and an individual having experience in public administration or policy, law enforcement, public finance or any other relevant field.⁵⁸ Nor does it provide for discretion in adding of certain members from other disciplines if deemed fit (as given under the central rules),⁵⁹ though it does allow the state government, in consultation with the authority, to provide such officers necessary for efficient discharge of latter's function.⁶⁰

This model of regulation by the state also becomes desirable in light of previous experience, showing that in purely self-regulated bodies, digital platforms tend to err on the side of caution to avoid imposition of liability by the state by way of creation of “*overbroad guidelines*”,⁶¹ enabling its arbitrary application. For example, in 2017, many LGBTQ content creators on *YouTube* reported their videos being hidden when the “*restricted mode*” was enabled owing to their LGBTQ content (with no explicit content).⁶² More specifically, a Youtuber reported that her videos discussing bisexuality were restricted, whilst other videos discussing sexual content explicitly with no reference to bisexuality were not restricted (with the platform subsequently acknowledging an error in their system).⁶³ This ‘restricted mode’ feature was launched by YouTube in 2010, allowing users to restrict content involving “*profanity, sexual content, nudity or violence*”.⁶⁴ Though this was recognised as a technical error, this is an example of arbitrary application of the above-mentioned guidelines by way of subjective interpretation of the said terms.

C. The Promotion and Regulation of Online Gaming Act 2025

⁵⁷ TN Online Gaming Act, s 3(2).

⁵⁸ IT Intermediary Rules, r 4A(2)(d).

⁵⁹ *ibid* r 4A(2)(d)(viii).

⁶⁰ TN Online Gaming Act, s 3(4).

⁶¹ Nimesh Singh, ‘Newly Regulated Digital Platforms And Self-Regulation: Exploring the Feasibility of the Mechanism’ (*Law School Policy Review*, 16 May 2023) <https://lawschoolpolicyreview.com/2023/05/16/newly-regulated-digital-platforms-and-self-regulation-exploring-the-feasibility-of-the-mechanism/#_ftn13> accessed 8 December 2024.

⁶² Clare Southerton and others, ‘Restricted modes: Social media, content classification and LGBTQ sexual citizenship’ (2021) 23(5) *New Media & Society* <<https://journals.sagepub.com/doi/epub/10.1177/1461444820904362>> accessed 9 December 2024.

⁶³ *ibid* 923-924.

⁶⁴ *ibid* 923.

On 22nd August last year, the 2025 Act received presidential assent. This act divides games into three categories.⁶⁵

First is an “online money game” which is defined as “an online game, irrespective of whether such game is based on skill, chance, or both, played by a user by paying fees, depositing money or other stakes in expectation of winning which entails monetary and other enrichment in return of money or other stakes; but shall not include any e-sports”.⁶⁶ Elaborating on what such “other stakes” are, the act defines it as “anything recognised as equivalent or convertible to money and includes credits, coins, token or objects or any other similar thing, by whatever name called and whether it is real or virtual, which is purchased by paying money directly or by indirect means or as part of, or in relation to, an online game”.⁶⁷

Second is an “online social game” which encompasses the following kinds of games:⁶⁸

- (i) Those not involving monetary or other stakes or any participation with the expectation of winning in the form of “monetary gain” in exchange of “money or other stakes”
- (ii) Those playable upon payment of a “subscription” or “one-time access” fee as long as the same is not in the form of a “stake or wager”
- (iii) Those offered only for “entertainment, recreation or skill-development”
- (iv) Those which do not fall within the category of an “online money game or e-sport”

Third are those games categorized as an “e-sport”, which are:⁶⁹

- (i) Those which are “played as part of multi-sports events”
- (ii) Those for which competitive events between teams or individuals are organized in multiplayer mode and are governed by a set of pre-determined rules
- (iii) Those recognised under the *National Sports Governance Act 2025* and registered with the authority or agency under Section 3 of the said act
- (iv) Those whose result is exclusively governed by a user’s skill (like physical dexterity, mental agility, strategic thinking and other similar skills)
- (v) Those which charge a fee in order to participate in such competition or to cover administrative costs (including “performance-based prize money”)

⁶⁵ ibid ss (2) (c), (2) (g), (2) (j), (2) (i).

⁶⁶ ibid s (2) (g).

⁶⁷ ibid s (2) (j).

⁶⁸ ibid s (2) (i).

⁶⁹ ibid s (2) (c).

- (vi) Those not involving placing of “*bets, wagers or any other stakes*” by anyone (irrespective of whether they are a participant or not), including winnings from the same

As this act seeks to regulate online games of chance,⁷⁰ just like for the 2023 Amendment, there has also been debate surrounding this legislation with regards to the potential of the same to intrude into the legislative domain of the state legislatures⁷¹ as provided for under the 7th Schedule of the constitution. The arguments presented for the 2023 Amendment pertaining to the State List containing wagers, sports and entertainment, digitization of once offline activities, as well as the rulings in *Bharat Shanti Lal Shah* (supra) and *State of Karnataka* (supra) are applicable here as well.

In terms of the regulatory structure, the 2025 Act provides for an authority (consisting of a chairperson and other members appointed by the centre) to oversee the implementation of its provisions of the act.⁷² This is a similar model as in the case of Tamil Nadu whereby regulation is entirely done by the state. One of the reasons mentioned behind shifting from a self-regulatory to a state regulation model is the non-operationalization of the self-regulatory bodies under the 2023 Amendment, leading to reconsideration of the regulatory framework itself.⁷³

III. REDEFINING ‘ONLINE GAMES OF CHANCE’

The regulatory structure as well as the definitions under the 2025 Act and the 2021 Act play a crucial role in how the statutory provisions and their rules are interpreted and applied. This role of interpreting the same becomes even more crucial in light of the dynamic nature of game designs, which present new and unique challenges and require striking a balance between supporting the online gaming industry whilst simultaneously promoting user welfare. One such challenge is of tackling addiction amongst users of online games, particularly from gambling-like design elements which do not involve real world currency. In this regard, this part of the paper will examine the potential limitations and ambiguities in the present regulatory regime in tackling such design elements which do not necessarily involve real-world financial

⁷⁰ Press Information Bureau, ‘Promotion and Regulation of Online Gaming Bill, 2025’ (Press Release No. 155075, 2025) <<https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155075&ModuleId=3®=1&lang=1>> accessed 3 January 2026; *ibid*; *ibid* ch III, IV V, VI.

⁷¹ Imran Fazal, ‘Centre vs State row erupts over Online Gaming Act as Chess player moves SC, terms it ‘colourable exercise of power’” (*Storyboard 18*, 1 November 2025) <<https://www.storyboard18.com/gaming-news/centre-vs-state-row-erupts-over-online-gaming-act-as-chess-player-moves-sc-terms-it-colourable-exercise-of-power-83563.htm>> accessed 1 December 2025.

⁷² Online Gaming Act, ch IV.

⁷³ Nakul Batra and others, ‘Legal Update- Promotion & Regulation of Online Gaming Bill, 2025’ (*Dsk Legal*, 22 August 2025) <<https://dsklegal.com/pro/>> accessed 6 October 2025.

transactions. This also entails drawing comparisons between the health effects of real-world and simulated gambling.

There exists a large variety of design techniques which involve simulated gambling. One such method to involve this element of chance is by incorporation of “*loot boxes*” which can be purchased using in-game currency.⁷⁴ This holds similarity to gambling in the sense that the contents of such boxes are decided at random and not known prior to their purchase.⁷⁵ Resultantly, this has led to loot boxes being banned in several countries.⁷⁶ Such a chance element however, is not limited to loot boxes but rather is part of broader “*random reward mechanisms*” (“RRM”) deployed in online games.⁷⁷ These mechanisms entail a chance of receiving a particular reward upon meeting certain conditions like completing a certain task, exceeding a particular playtime, etc.⁷⁸

Furthermore, such designs can be considered to be dark patterns. This is because, dark patterns and addictive design elements are not completely separate and isolated concepts. In fact, the argument that addictive design elements can be categorised as a dark pattern is not new but rather has previously been adopted by the *Spanish Data Protection Agency* (“SDPA”) which mentioned all “*addictive patterns*” to fall within the category of “*deceptive patterns*” (but not necessarily vice-versa).⁷⁹ With a report released by the *OECD* mentioning that those dark patterns which “*sufficiently capture the consumer’s attention and time for extended durations*” being considered addictive.⁸⁰ In this context, the report also mentions that loot boxes incorporate addictive patterns and are considered to be a kind of “*gambification*” due to similarities with slot machines.⁸¹ More broadly, RRM and gambling design elements can also

⁷⁴ Thomas de Haan, ‘Dark Patterns In Games: How Do They Influence Players’ Experiences And Their Willingness To Give Up Personal Information?’ (Bachelor Thesis, Radboud University 2022), 16 <https://www.cs.ru.nl/bachelors-theses/2022/Thomas_de_Haan___1024718___Dark_patterns_in_games_-_how_do_they_influence_player_experiences_and_their_willingness_to_give_up_personal_information.pdf> accessed 5 November 2025.

⁷⁵ *ibid.*

⁷⁶ *ibid.*

⁷⁷ Department For Culture, Media And Sport, *Loot Boxes and digital gaming: a rapid evidence assessment* (2021) 5, 42.

⁷⁸ Michael Yin and Robert Xiao, ‘The Reward for Luck: Understanding the Effect of Random Reward Mechanisms in Video Games on Player Experience’ (*CHI’22: CHI Conference on Human Factors in Computing Systems, New Orleans*, April 2022) <https://robertxiao.ca/pubs/2022_CHI_RewardForLuck.pdf> accessed 24 June 2025.

⁷⁹ Agencia Española De Protección De Datos, ‘Addictive patterns in the processing of personal data’ (*Agencia Española De Protección De Datos*, 2024) <<https://www.aepd.es/guides/addictive-patterns-in-processing-of-personal-data.pdf>> accessed 2 December 2025.

⁸⁰ Organisation For Economic Co-Operation and Development, ‘*Dark Commercial Patterns*’ (DSTI/CP(2021)12/FINAL, Organisation for Economic Co-Operation and Development, 2022) 25 <[https://one.oecd.org/document/DSTI/CP\(2021\)12/FINAL/en/pdf](https://one.oecd.org/document/DSTI/CP(2021)12/FINAL/en/pdf)> accessed 24 June 2025.

⁸¹ *ibid* 26.

be considered to be dark patterns⁸²(though there is literature challenging such a characterization of gambling).⁸³

In the introduction of this paper, it was mentioned that governments regulate the manufacture, sale and distribution of various substances considered to be addictive through various legislations.⁸⁴ In the context of online games, game developers incorporate *RRMs* which aid in creation of repetitive behaviours⁸⁵ [using the “*intermittent reinforcement*” model, by occasionally providing the player with rare items (though used in the context of loot boxes,⁸⁶ can be applied to rare boss drops of Massively Multiplayer Online Role-Playing (“MMORPG”) games too owing to the structural similarity of the two models, i.e., randomized chance to receive a rare item upon completion of each boss fight/opening of a loot box)],⁸⁷ thereby encouraging a behavioural loop which keeps the user hooked. Furthermore, such mechanisms can serve as an added risk for future gambling addiction.⁸⁸

Such behavioural addictions like gambling (a similar mechanism has been incorporated in MMORPG games)⁸⁹ and internet addiction have been found to be similar to drug addiction with the only major difference being, that in case of the former, the user is not addicted to a particular substance but rather the feeling derived from engaging in the said behaviour.⁹⁰ Furthermore, almost all of the proposed criteria for internet gaming disorder are analogous to

⁸² Michal Jastrzebski and Jakob Ek, ‘Dark Patterns Within Gacha Games’ (Bachelor Thesis, Blekinge Institute of Technology 2024), 9 <<http://www.diva-portal.org/smash/get/diva2:1888600/FULLTEXT01.pdf>> accessed 11 October 2025; Jacob Aagaard and others, ‘A Game of Dark Patterns: Designing Healthy, Highly-Engaging Mobile Games’ in Simone Barbosa, Cliff Lampe, Caroline Appert and David A. Shamma (eds), *CHI EA’22: Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery, 2022).

⁸³ Scott A. Goodstein, ‘When The Cat’s Away: Techlash, Loot Boxes, And Regulating “Dark Patterns” In The Video Game Industry’s Monetization Strategies’ (2021) 92 University Of Colorado Law Review, 300 <<https://lawreview.colorado.edu/wp-content/uploads/2021/03/Goodstein.pdf>> accessed 11 October 2025.

⁸⁴ Delhi Act, s 23.; Delhi Rules, r 51(1).; MP Act, s 23.

⁸⁵ Digital, Culture, Media And Sport Committee, *Immersive and addictive technologies*, (HC 2017-19, 1846) para 127

⁸⁶ Alexandra Puhm and others, ‘Risks and Harms associated with Online Gaming and Gambling’ (*Council Of Europe International Co-Operation Group on Drugs And Addictions*, 2024) 17 <<https://rm.coe.int/p-pg-it-2024-2-report-risks-and-harms-online-gaming-and-gambling-final/1680b07d35>> accessed 29 December 2024.

⁸⁷ Sri Bharadwaj Tolety, ‘Correlation Between Player Type and Design Features of MMORPGs And Loot Systems’ (*Masters Thesis Northeastern University*, 2019) 21-22. <<https://repository.library.northeastern.edu/files/neu:m0455c898/fulltext.pdf>> accessed 2 December 2025; John Woodhouse, ‘Loot boxes in video games’ (House Of Commons Library, 2024), 6 <<https://researchbriefings.files.parliament.uk/documents/CBP-8498/CBP-8498.pdf>> accessed 24 January 2025.

⁸⁸ Andrew Shenberg, ‘Betting on the Future: Regulating Microtransactions in Video Games and Proposing Comprehensive Consumer Protections’ (2025) 69(2) New York Law School Law Review 144 <https://digitalcommons.nyls.edu/cgi/viewcontent.cgi?article=2720&context=nyls_law_review> accessed 11 October 2025.

⁸⁹ Tolety (n 91) 11, 27, 44.

⁹⁰ Seyyed Salman Alavi and others, ‘Behavioral Addiction versus Substance Addiction: Correspondence of Psychiatric and Psychological Views’ (2012) 3(4) International Journal Of Preventive Medicine 291 <<https://pmc.ncbi.nlm.nih.gov/articles/PMC3354400/>> accessed 2 January 2025.

those symptoms used to diagnose issues under DSM-5 SUD (relating to drug addiction), like fixation on the material concerned⁹¹ (though, there exists a body of literature critiquing the usage of same criteria for drug and gaming addiction citing the irrelevance of symptoms like withdrawal, mood regulation, etc. for problematic gaming).⁹²

There exist multiple similarities between drug addiction and gaming addiction. Both narcotics and gaming result in release of dopamine from the brain which has been suggested to play a role in addictive behaviours,⁹³ with studies showing similar neural processes occurring for gaming and substance addicts, with increased activity being recorded in the part of the brain (of gaming addicts) usually associated with substance addictions.⁹⁴ A study has also found a link between the frequency of gaming and substance abuse.⁹⁵

Furthermore, such similarities between gaming and gambling addictions to drug addiction make it important to examine whether certain design elements that are structurally similar to gambling (irrespective of whether there exists a monetary element or not), increase the risk of future gambling addiction.⁹⁶

A. Non-Monetary Gambling

Griffiths and Meredith (2009), point out that video games can be considered to be a non-monetary form of gambling, whereby players can play for in-game points rather than real-life currency⁹⁷ (with repetitive gambling, having the potential to turn into gambling disorder,⁹⁸ i.e.,

⁹¹ Kenneth L. Smith, Tom A. Hummer and Leslie A. Hulvershorn, 'Pathological Video Gaming and Its Relationship to Substance Use Disorders' (2015) 2 *Current Addiction Reports* 303 <<https://link.springer.com/article/10.1007/s40429-015-0075-6>> accessed 1 January 2025.

⁹² Alexandra Infanti and others, 'Gaming passion contributes to the definition and identification of problematic gaming' (2023) 147, *Addictive Behaviours* 2 <<https://www.sciencedirect.com/science/article/pii/S0306460323002009>> accessed 26 October 2024.

⁹³ Giusi Antonia Toto and Pierpaolo Limone, 'Signs, mechanisms and consequences of videogame addictions: educational strategies and rehabilitation' (Technology Enhanced Learning Environments for Blended Education-The Italian e-Learning Conference, Vieste, June 2022) <https://ceur-ws.org/Vol-3265/paper_4924.pdf> accessed 11 October 2025.

⁹⁴ Marloes L.C. Spekman and others, 'Gaming addiction, definition and measurement: A large-scale empirical study' (2013) 29(6) *Computers in Human Behaviour*, 2151. <https://www.researchgate.net/publication/241707285_Gaming_addiction_definition_and_measurement_A_large-scale_empirical_study> accessed 2 January 2025.

⁹⁵ Maxine M. Denniston and others, 'Associations between Electronic Media Use and Involvement in Violence, Alcohol and Drug Use among United States High School Students' (2011) 12(3) *Western Journal Of Emergency Medicine: Integrating Emergency Care With Population Health*, 313 <<https://escholarship.org/uc/item/66s8b252>> accessed 2 January 2025.

⁹⁶ *Shenberg* (n 92).

⁹⁷ Ulric Wong and David Carson Hodgins, 'Development of the game addiction inventory for adults (GAIA)' (2013) 22(3) *Addiction Research and Theory* 2 <<https://ucalgary.ca/sites/default/files/teams/252/Gaming%20Addiction%20Inventory%20for%20Adults%20Manuscript.pdf>> accessed 4 January 2025.

⁹⁸ 'Addictive behaviour' (*World Health Organization*) <https://www.who.int/health-topics/addictive-behaviour#tab=tab_1> accessed 1 January 2025.

gambling addiction).⁹⁹ An example of this can be seen in the structure of MMORPG games, wherein users spend time killing a specific boss in the hopes of receiving a random reward¹⁰⁰ (with the ‘drop rate’, i.e., the “*frequency at which rewards drop*” being varied owing to such randomness).¹⁰¹ This repeated killing of a boss in hopes for a specific reward is how users are kept hooked¹⁰² (as varied rewards generate interest),¹⁰³ leading to game developers to use a dark pattern known as “*Grinding*”, which include game mechanics requiring the users to perform “*repetitive and tedious tasks*”.¹⁰⁴ The present regulation of dark pattern, by the definition of ‘dark pattern’, seeks to regulate ‘deceptive’ design and not necessarily behaviour modifying designs.¹⁰⁵ This dichotomy between awareness and compulsiveness was also recognised by the *European Parliament*, who mentioned that their *Digital Services Act* does include provisions to combat dark patterns, however the same are restricted to only include “*choice architecture*” and “*influence choices*” and does not specifically address addictive designs.¹⁰⁶

The above-mentioned example of variable reward has been incorporated into loot boxes as well. These are items which can be obtained through in game play or purchase,¹⁰⁷ which offer players a reward which is determined by chance.¹⁰⁸ This is important because, according to *B.F. Skinner*, even predicting outcomes can lead to release of dopamine.¹⁰⁹ In 2018, the *Belgium*

⁹⁹ ‘Gambling Disorder’ (*American Psychiatric Association*) <<https://www.psychiatry.org/patients-families/gambling-disorder>> accessed 1 January 2025

¹⁰⁰ Seth A. Brimley, ‘Game Over, Loot Boxes: Insert Self-Regulation to Continue 10..9..8..7..’, (2020) *Arizona Legal Studies*, 14 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3585551> accessed 12 October 2025.

¹⁰¹ *Tolety* (n 91) 9.

¹⁰² Romario Verbran, ‘[Game UX Case] How I raised an MMO’s player base by 70%’ (*Medium*, October 3 2022) <<https://romarioverbran.medium.com/game-ux-case-how-i-raised-an-mmos-player-base-by-70-f2f414fdf9f>> accessed 29 December 2024.

¹⁰³ Nir Eyal and Ryan Hoover, *Hooked: How To Build Habit-Forming Products* (CreateSpace Independent Publishing Platform, 2013) 9.

¹⁰⁴ José P. Zagal, Staffan Björk and Chris Lewis, ‘Dark Patterns in the Design of Games’ in Georgios N. Yannakakis, Espen Aarseth, Kristine Jørgensen and James C. Lester (eds), *Proceedings of the 8th International Conference on the Foundations of Digital Games* (Society for the Advancement of the Science of Digital Games 2013).

¹⁰⁵ Guidelines for Prevention and Regulation of Dark Patterns 2023, F. No. CCPA-1/1/2023-CCPA-(Reg)., cl 2(1)(e).

¹⁰⁶ This resolution also recognised the limited scope of the regulations, mentioning the same to only cover online platforms and not online games. See European Parliament, ‘Addictive design of online services and consumer protection in the EU single market’ (P9_TA(2023)0459, 2019-24, European Parliament, 2023), para P. <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.pdf> accessed 22 September 2025

¹⁰⁷ Elijah Tredup, ‘Loot Boxes And The Question Of Gambling’ (Nevada Gaming Lawyer, 2019), 59 <<https://nvbar.org/wp-content/uploads/13-Loot-Boxes.pdf>> accessed 8 November 2025.

¹⁰⁸ Stuart Gordon Spicer and others, ‘Loot boxes and problem gambling: Investigating the “gateway hypothesis”’ (2022) 131 *Addictive Behaviors*, 1 <<https://www.sciencedirect.com/science/article/pii/S0306460322000934>> accessed 2 January 2025.

¹⁰⁹ Alberto Monge Roffarello, Kai Lukoff and Luigi De Russis, ‘Defining and Identifying Attention Capture Deceptive Designs in Digital Interfaces’ in Albrecht Schmidt, Kaisa Väänänen, Tesh Goyal, Per Ola Kristensson,

Gaming Commission, found that paid loot boxes have the constituent elements of ‘gambling’, i.e., “game, wager, chance, win/loss” which are similar to ‘games of chance’,¹¹⁰ pursuant to which a ban on loot boxes was imposed.¹¹¹ This made *Belgium* part of a group of countries globally to regulate/ban loot boxes.¹¹² Applying the above criteria used by the *Belgium Gaming Commission*, it can be argued that in boss fights in MMORPG games, users wager their time and resources for a chance to get a rare drop. The need to regulate such addictive game design, which, basis the above discussion (on “drop rate”), which can be said to be structurally similar to gambling, becomes more apparent with studies showing users engaging in online gambling (particularly those with certain difficulties) have a higher risk to their physical health as compared to those who engage in gambling at physical establishments.¹¹³

While the 2023 amendment to the Intermediary Guidelines does mandate self-regulatory bodies to ensure their framework contains measures to combat addiction, such a rule is only applicable for verifying an “online real money game”,¹¹⁴ which is defined as an online game wherein a user deposits money or kind¹¹⁵ (clarity is still required on what would constitute ‘kind’ in the context of a ‘real money game’)¹¹⁶ and hence may not apply to non-monetary loot boxes (offering in-game items) or all kinds of addictive game design¹¹⁷ (as mentioned above, *Griffiths and Meredith* opined that gambling can be non-monetary as well).¹¹⁸ Regarding such addictive game design, it is important to note that such items may be obtained through the ‘drop rate’ mechanism as well.¹¹⁹

Anicia Peters, Stefanie Mueller, Julie R. Williamson, Max L. Wilson (eds), CHI’23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (Association for Computing Machinery 2023).

¹¹⁰ Gaming Commission, ‘Research Report on Loot Boxes’ (Gaming Commission, 2018), 16 <<https://www.gamingcommission.be/sites/default/files/2021-08/onderzoeksrapport-loot-boxen-Engels-publicatie.pdf>> accessed 1 December 2025.

¹¹¹ Tom Gerken, ‘Video game loot boxes declared illegal under Belgium gambling laws’ *British Broadcasting Corporation* (April 26, 2018) <<https://www.bbc.com/news/technology-43906306>> accessed 1 January 2025

¹¹² ‘A look at the current state of videogame loot box regulation worldwide’ (*ID3 Digitech*, 30 August 2023) <<https://www.id3.com/blog/loot-box-regulation-worldwide>> accessed 1 January 2025.

¹¹³ Puhm and others (n 90) 18.

¹¹⁴ IT Rules Amendment, r 6.

¹¹⁵ *ibid* r 2(ii).

¹¹⁶ Rachit Bahl, Sumit Ghoshal and Arjun Uppal, ‘Online Gaming: Game On or Game Over?’ (*Azb & Partners*, 1 May 2023) <<https://www.azbpartners.com/bank/online-gaming-game-on-or-game-over/>> accessed 1 January 2025.

¹¹⁷ Swarndeeep Singh and Yatan Pal Singh Balhara, ‘Rules for Online Gaming Regulation in India: The Endgame or We Need to Level Up?’ (2024) 46(6) *Indian Journal Of Psychological Medicine*, 590 <https://pmc.ncbi.nlm.nih.gov/articles/PMC11558710/pdf/10.1177_02537176231206938.pdf> accessed 19 January 2025.

¹¹⁸ Text to n 101 in Part III.A.

¹¹⁹ Brimley (n 104) 28.; Tolety (n 91) 9.

Also, while loot boxes may seem like gambling in online games, they are designed in a manner so as to elude the legal definition of ‘gambling’ in various statutes.¹²⁰ In India, for example, the Intermediary Guidelines focus on existence of a straightforward “*deposit-to-winning relationships*”.¹²¹ The problem with this approach is that it may not regulate instances which covert real-world currency into multiple forms (like using real world currency to purchase virtual currency which can in turn be used to purchase loot boxes).¹²² This then makes it difficult to draw a direct link between deposits of real-world currency and rewards based on chance¹²³ and be “*highly lucrative*” for developers.¹²⁴

More specifically, in the context of MMORPG games, clarity is needed on whether attainment of superior weapons and armour (by any means) for the purpose of ensuring successful completion of ‘boss fights’ would be considered to be a deposit ‘in kind’. Furthermore, these regulations seek to regulate the monetary aspect and the addiction arising out of the same. However, as already mentioned, game designs, like gambling on drop rates in MMORPGs, without necessarily spending any money can also be addictive (applying *B.F. Skinner’s* theory mentioned above).¹²⁵ This need to regulate such non-monetary gambling becomes even more apparent in the Indian context, with various literature indicating a majority of online gaming players in India to be Free-To-Play users.¹²⁶

While the above debate was ongoing, the notification of the 2025 Act introduced new dimensions to the above problem. The same arise out of the definitions of “*online money game*” and “*other stakes*” under the said act. From a joint reading of their definitions, it is evident that the same have been worded in a broad manner. The definition of ‘other stakes’ does seem to improve upon the lacuna with the Intermediary Guidelines mentioned above (regarding being focused on a straightforward “*deposit-to-winning*” relationship)¹²⁷ by

¹²⁰ Goodstein (n 87) 290-291.;

Albert Pou Puertas, ‘Decoding Random Virtual Rewards: A Guide To Identify Hazard Game Design Techniques In Video Games’ (Bachelor Thesis, Polytechnic University of Catalonia 2023), 58 <<https://share.google/LG0aftbv4eEJKO05F>> accessed 2 December 2025.

¹²¹ Aman Gupta and Samriddh Sharma, “‘The Cake is a Lie:’ Locating Loot Boxes in India Gaming Framework’ (2025) 20(1) Indian Journal Of Law And Technology, 169 <<https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1557&context=ijlt>> accessed 5 October 2025.

¹²² *ibid.*

¹²³ *ibid.*

¹²⁴ Puertas (n 124).

¹²⁵ Roffarello, Lukoff and Russis (n 113).

¹²⁶ Rajesh Dhuddu and others, ‘From sunrise to sunshine: The contribution of online gaming to the Viksit Bharat journey and India’s cultural power’ (PricewaterhouseCoopers, 2024), 23 <<https://www.pwc.in/assets/pdfs/online-gaming-to-the-viksit-bharat-journey-old.pdf>> accessed 9 January 2025; Rameesh Kaliasam and Priyanka Mathur, ‘Online Fantasy Sports: Adding Value to the Indian Sporting Ecosystem’ (IndiaTech.Org, 2020), 2 <<https://www.indiatech.org/wp-content/uploads/2020/09/IndiaTech.org-Whitepaper-OnlineFantasySports-compressed.pdf>> accessed 30 September 2025.

¹²⁷ Gupta and Sharma (n 125).

regulating purchase of virtual currency using real-world currency directly or by any indirect means.

However, the definition of ‘online money game’ still makes mention of a “*deposit*” which can be in real world or virtual currency. Applying the example of MMORPG games mentioned above, it remains to be seen whether the same would be interpreted in a manner whereby purchase of weapons using in-game currency (obtained via gameplay) for successful and/or efficient completion of a boss fight (resulting in a reward basis the ‘drop rate’) would be considered to be a ‘deposit of other stakes made in expectation of enrichment of other stakes’. This ambiguity is also because of the fact that the act was notified only recently on 22nd August 2025, with its rules (“**2025 Rules**”) still in the draft stage,¹²⁸ and with the constitution of the Online Gaming Authority pending. Therefore, the manner in which the said act and its rules are interpreted is an open-ended question for now.¹²⁹ This obscurity is further enhanced by the criteria laid down for determination of an online game under the 2025 Rules. More specifically, the parameter laid down under Rule 13(1)(b) entails determining whether such ‘deposit’ is used as a “*consideration for winning*”.¹³⁰

Furthermore, Rule 13(1)(d) entails an examination of whether the online games for which deposits have been made provide for any reward through money or “*other enrichment*” which can be encashed as money. A potential issue which may arise here is of *Real World Trading*. This refers to the practice of conversion of in-game assets for real-world currency.¹³¹ While the game itself may not provide an option of such encashment, it may be nonetheless enabled by third parties. This practice has been banned by many games already by making users agree to an *End User License Agreement* (EULA), whereby a user waives their right to claim ownership over their virtually generated assets.¹³² However, it continues to take place beyond the control of game developers on third-party websites.¹³³ This is because, looking at the experience in

¹²⁸ ‘Promotion and Regulation of Online Gaming Act 2025 and Its Corrigenda’ (*Ministry of Electronics and Information Technology*) <<https://www.meity.gov.in/documents/act-and-policies/promotion-and-regulation-of-online-gaming-act-2025-and-its-corrigenda-kTMxQjMtQWa>> accessed 8 October 2025.

¹²⁹ Mentioned in the context of loot boxes and gacha game mechanics but is relevant here owing to their similarity to drop rates. See Rayan Sayyed, ‘India’s Online Gaming Bill Leaves Loot Boxes and Gacha Mechanics in a Grey Zone for Video Games’ (*IGN*, 1 September 2025) <<https://in.ign.com/policy/240431/editorial/indias-online-gaming-bill-leaves-loot-boxes-and-gacha-mechanics-in-a-grey-zone-for-video-games>> accessed 8 October 2025.

¹³⁰ The Promotion and Regulation of Online Gaming Rules 2025, r 13 (1) (b).

¹³¹ Atsushi Fujita, Hiroshi Itsuki and Hitoshi Matsubara, ‘Detecting Real Money Traders in MMORPG by Using Trading Network’ in Vadim Bulitko and Mark Riedl (eds), *Proceedings, The Seventh AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment* (AAAI Press, 2011).

¹³² Augustus Urschel, ‘Understanding Real Money Trading in MMORPGs’ (2011) *New World Disorder*, 8 <<https://scholarspace.library.gwu.edu/downloads/kd17ct08j?disposition=inline&locale=en>> accessed 5 October 2025.

¹³³ Environment And Communications References Committee, *Gaming micro-transactions for chance-based items* (Senate, 2018) para 2.51.

other jurisdictions, taking legal actions against such websites by game developers does run into difficulties at times.¹³⁴ For example, in South Korea, in a decision early as 2002, a District Court refused grant of preliminary injunction against websites auctioning in-game items on the ground that the terms of service restricting a user's right of intellectual property over their in-game items cannot be extended to such auction websites not party to the said terms.¹³⁵

Another change with the 2025 Act and its rules is a shift in linking chance-based games with money unlike in the Intermediary Guidelines. In the context of the problems discussed above regarding the pre-2025 regulations, the problem of linking the definition of 'gambling' with usage of real currency is not unique to India. In Denmark, the *Danish Gambling Authority* drew a distinction between the loot boxes incorporated in *Star Wars Battle Front* and "skin betting" in *Counter-Strike: Global Offensive* when it came to classifying them as 'gambling'.¹³⁶ The authority argued that the former is not gambling owing to difficulty in conversion of such loot boxes for real-world currency.¹³⁷ For the latter, the authority argued the same to be gambling owing to ease of conversion of the skins into real-world currency.¹³⁸

This stance however, overshadows the similar health consequences of games with mechanisms structurally similar to gambling (for example, RRM),¹³⁹ irrespective of the involvement of real-world currency. This becomes particularly problematic for two reasons. *First*, it ignores the fact that there is growing evidence that the health effects resulting from such gambling-like game designs and real gambling are similar¹⁴⁰ (like increased tolerance in the form of "excessive screen times" and risk of development of "problematic gambling"¹⁴¹ for the former and risk of development of such problem gambling, leading to higher probability of increased frequency of gambling for the latter).¹⁴² *Second*, such "stimulated gambling" can serve as a

¹³⁴ Ung-gi Yoon, 'Real Money Trading in MMORPG Items From a Legal and Policy Perspective' (2008) 1(1) Journal Of Korean Judicature <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1113327> accessed 6 October 2025.

¹³⁵ *ibid.*

¹³⁶ *Puertas* (n 124) 28.

¹³⁷ *ibid.*

¹³⁸ *ibid.*

¹³⁹ *ibid* 32.

¹⁴⁰ Standing Committee On Social Policy And Legal Affairs, *You win some, you lose more- Report of the inquiry into online gambling and its impacts on those experiencing gambling harm* (HR 2022-25) paras 6.10, 6.13

¹⁴¹ Nerilee Hing and others, 'Adolescents Who Play and Spending Money in Simulated Gambling Games Are at Heightened Risk of Gambling Problems' (2022) 19(17) International Journal Of Environmental Research And Public Health, 12 <<https://pmc.ncbi.nlm.nih.gov/articles/PMC9517771/pdf/ijerph-19-10652.pdf>> accessed 12 October 2025.

¹⁴² 'FAQs: What is Problem Gambling?' (*National Council On Problem Gambling*) <<https://www.ncpgambling.org/help-treatment/faqs-what-is-problem-gambling/>> accessed 11 January 2026; Shawn R. Currie and others, 'Risk of Harm among Gamblers in the General Population as a Function of Level of Participation in Gambling Activities' (2006) 101(4) Addiction 3 <<https://jogoremoto.pt/docs/extra/OrboN7.pdf>> accessed 13 October 2025.

gateway for gambling using real-world currency (through factors like learning, confidence and an urge to gain real-world currency).¹⁴³

This problem of regulation of only those games which involve real life currency extends to the guidelines issued by the *Advertising Standards Council of India* in 2020 (which were also cited in an advisory issued by the *Union Ministry of Information and Broadcasting* on the subject of advertisements of online games),¹⁴⁴ which imposed a duty to warn about the financial risks and addictive nature of the game on the advertisers of the game.¹⁴⁵ However, the said rules were only applicable to advertisement of games involving real-life monetary winnings¹⁴⁶ and do not cover all forms of addictive games. In this regard, it was reported in 2024 that the government was considering imposing monetary and time limits for online game users,¹⁴⁷ after which the 2025 Act was introduced last year.

Basis the above discussion surrounding the uncertainty at this stage of how the regulations under the 2025 Act and its rules will be interpreted in the context of attainment of weapons for boss fights and the drop rate mechanism for such fights, the regulation of various forms of RRM by way of an interpretation of the 2025 Act and its rules also remains an open-ended question as of now.

B. Approach Taken by Tamil Nadu

The preamble of the TN Gaming Act, in laying down the objects and reasons behind the legislation, recognises the need to tackle gaming addiction as well as the harms caused both to the health (including a mention of the recognition of gaming disorder by the *World Health Organisation*) and financial condition of an individual.¹⁴⁸

The act identifies four kinds of games to be considered as an “*online game of chance*”:¹⁴⁹

- (a) Contains both an element of chance and skill, with the former overshadowing the latter
- (b) Contains an element of chance which can only be removed via a superlative skill

¹⁴³ Nerilee Hing and others, “It Doesn’t Give Off the Gambling Vibes....It Just Feels Like a Part of the Game’: Adolescents’ Experiences and Perceptions of Simulated Gambling While Growing Up’ (2025) 23(1) *International Journal Of Mental Health And Addiction*, 405 <<https://link.springer.com/article/10.1007/s11469-023-01119-6>> accessed 4 October 2025.

¹⁴⁴ Ministry of Information and Broadcasting, *Advisory on Advertisements on Online Gaming, Fantasy Sports, etc.* (Advisory, 4407/13/2019-BC-I, 2020) <https://mib.gov.in/sites/default/files/2024-02/Advisory%20on%20online%20betting%20advertisements%2013.06.2022%282%29_0%20%281%29.pdf> accessed 13 January 2025.

¹⁴⁵ *ibid* 5.

¹⁴⁶ *ibid*.

¹⁴⁷ Aashish Aryan, ‘Govt eyes time, spend curbs to tackle gaming addiction’ *The Economic Times* (May 29, 2024) <<https://economictimes.indiatimes.com/tech/technology/govt-eyes-time-spend-curbs-to-tackle-gaming-addiction/articleshow/110505799.cms?from=mdr>> accessed 8 December 2024.

¹⁴⁸ TN Online Gaming Act, Preamble.

¹⁴⁹ *ibid* s 2(1).

(c) Game presented to involve an element of chance

(d) Contains any device operating on a random outcome generator

In the context of the discussion on *MMORPG* games above, the mechanism surrounding drop rates and its related effects can be said to be characteristic of a device which operates on a random outcome generator.¹⁵⁰ This definition becomes important, as it recognizes such game designs to be ‘games of chance’ irrespective of involvement of any monetary element (as stated above, the legislature in enacting the act, recognized both the health hazard as well as the negative financial implications of gaming addiction)¹⁵¹ and hence would address the issue raised by *Griffith and Meredith* pertaining to ‘non-monetary gambling’ mentioned above.¹⁵² Furthermore, the act places a general prohibition on playing games listed in its schedule with money or any other form of stake.¹⁵³ The latter part (‘any other form of stake’) becomes important in the context of the above-mentioned discussion on ‘non-monetary gambling’ and is similar to the definition of ‘online real money game’ under the 2023 amendment which identifies deposits to not only exist in money but also in kind¹⁵⁴ (though, as stated above, clarity is needed on what constitutes ‘kind’ in this context,¹⁵⁵ including in this state legislation). While the definition does have a wide ambit, the schedule of the act which lists the kinds of prohibited games of chance, only categorizes rummy and poker as being “*online games of chance*” and does not address specific game designs (with certificate of registration being contingent on non-hosting of games specified in schedule).¹⁵⁶ Though, it is important to note that the *Madras High Court* in 2023, declared the decision to include rummy and poker as “*online game of chance*” as ultra vires,¹⁵⁷ pursuant to which the said decision was appealed to the *Supreme Court* and the matter is presently sub-judice.¹⁵⁸ However, irrespective of the said decision and pending appeal, this neutrality in defining the scope of ‘game of chance’ is something which can be incorporated within the 2025 Act (along with clarity on its scope), thereby making it applicable across the country (since digital communication is a central subject).¹⁵⁹

¹⁵⁰ *Tolety* (n 91) 9.

¹⁵¹ TN Online Gaming Act, Preamble.

¹⁵² *Wong and Hodgins* (n 101).

¹⁵³ TN Online Gaming Act, s 7 (2).

¹⁵⁴ IT Intermediary Rules, r 2(1) (qd).

¹⁵⁵ *Bahl, Ghoshal and Uppal* (n 120).

¹⁵⁶ *ibid* s 10(5)(a).

¹⁵⁷ *All India Gaming Federation vs State of Tamil Nadu and others* 2023 SCC OnLine Mad 6973 [123].

¹⁵⁸ *The State of Tamil Nadu vs All India Gaming Federation* SLP(C) 001588-001592/2024.

¹⁵⁹ Constitution, sch. VII, List I, Entry 31.

C. Games of 'skill' vs 'chance'

In India, there is no specific central legislation on gambling, with the *Public Gambling Act 1867* (which has been amended by various states),¹⁶⁰ which exempts games of “*mere skill*” from its ambit¹⁶¹ having been already repealed by various states¹⁶². However, the said legislation provides no definition of ‘gambling’ or ‘game of chance’ (or what constitutes ‘skill’), nor does it provide a framework to differentiate between ‘games of skill’ and ‘games of chance’. This void persists in other central legislations as well (like the Intermediary Guidelines). This incongruity in gambling laws also stems from the fact that ‘betting and gambling’ fall within the state list,¹⁶³ with different states coming up with different definitions of the same. In absence of such uniformity in the statutory definition of ‘game of chance’ and ‘game of skill’, different courts in India have considered the issue in a catena of precedents.

The *Supreme Court* has previously delineated the two above-mentioned concepts.¹⁶⁴ The court understood ‘games of chance’ as those determined entirely or partly via lot or mere luck, wherein the result is largely uncertain or doubtful with no person being capable of being certain of the outcome prior to the occurrence of the same.¹⁶⁵ Conversely, the court defined ‘games of skill’ as being one wherein a successful outcome is largely contingent on the “*superior knowledge, training, attention, experience and adroitness*” of the user (though, the court recognized that even in such kinds of games, the element of chance is not completely negated).¹⁶⁶ The distinction drawn in the said case can be understood in conjunction with the phrase “*mere skill*” mentioned under the *Public Gambling Act*, to mean that mere existence of an element of chance is insufficient to exempt it from regulation under the said act.

The *Supreme Court* in *M.J. Sivani and others v State of Karnataka and others*¹⁶⁷ interpreted the said phrase, acknowledging the no game is based on pure skill alone. The court added that when the element of chance gained preponderance in a game, then such a game cannot be categorized as one being of “*mere skill*”.

¹⁶⁰ Public Gambling (Madhya Pradesh Amendment) Act 1976; Public Gambling (Himachal Pradesh Amendment) Act 1976.

¹⁶¹ Public Gambling Act 1867, s 12.

¹⁶² The Haryana Prevention of Public Gambling Act 2025, s 18(1).; The Delhi Public Gambling Act 1955, s 18(1).

¹⁶³ Constitution, sch VII, List II, Entry 34.

¹⁶⁴ *Dr. K.R. Lakshmanan vs State of T.N. and Another* (1996) 2 SCC 226 [3].

¹⁶⁵ *ibid.*

¹⁶⁶ *ibid.*

¹⁶⁷ *M.J. Sivani and others v State of Karnataka and others* (1995) 6 SCC 289 [11].

In this regard, in 2023, the *Karnataka High Court* held that a game of skill, with or without stakes would not constitute ‘gambling’.¹⁶⁸ In the context of *MMORPG* games (and in the context of the acknowledgement made in *K.R. Lakshman* (supra) and *MJ Sivani* (supra) judgements about games of skill also having an element of chance), mechanisms pertaining to fighting ‘bosses’ can be considered to be one of ‘skill’ (as the ratio in *K.R. Lakshman* (supra) mentioned the successful outcome in games of skill to be largely contingent on the user’s “superior knowledge, training, attention experience and adroitness”), owing to the requirement of superior in-game items¹⁶⁹ and training. Furthermore, it has been previously observed, that for a game to be considered that of ‘skill’, such skill must control the final outcome of the game and not be part of a larger scheme.¹⁷⁰ In this regard, whilst these ‘skills’ of a player do play a role in determining whether or not the player prevails in the boss fight itself, it does not control the final outcome, i.e., the reward to be received by the player, which is governed by a random mechanism (known as “drop rate”).¹⁷¹ This mechanism, as discussed above, is structurally similar to gambling.

Since both loot boxes and drop rates function on the same concept, i.e., RRM,¹⁷² the ambiguity surrounding the former’s regulation under the Intermediary Guidelines is relevant here. The regulation of loot boxes is symptomatic of a larger lacuna in online gaming regulation in India, i.e., the failure to address “hybrid gaming mechanics”.¹⁷³ This arises from the binary assumption present under the said rules, i.e., that a game may be played exclusively for “entertainment” or for “winnings”.¹⁷⁴ This distinction is, however, not easily discernible for modern games which deploy complex monetization techniques like loot boxes, which combine the chance-based rewards provided by such a box with the otherwise skill-based or recreational nature of the game.¹⁷⁵ This drawback results in a mismatch between the scope of the regulation

¹⁶⁸ While this was in the context of the Central Goods and Services Tax Act 2017, it is still relevant as the judgement examined the difference between ‘games of skill’ and ‘games of chance. See *Gameskraft Technologies Private Limited vs Directorate General of Goods and Services Tax Intelligence (Headquarters) and Others (and other cases)* 2023 SCC OnLine Kar 18 [45].

¹⁶⁹ *Tolety* (n 91) 18.

¹⁷⁰ Naman Lohiya and Sakshi Pawar, ‘A Gamble Of Laws: Reconciling The Conflicting Jurisprudence On Gambling Laws In India’ (2019) 13(1) *Nalsar Student Law Review*, 57 <[https://nalsar.ac.in/images/NSLR-VOL.13\(1\).pdf](https://nalsar.ac.in/images/NSLR-VOL.13(1).pdf)> accessed 21 October 2025.

¹⁷¹ *Tolety* (n 91) 9.

¹⁷² Department For Culture, Media And Sport (n 81).; Arvinn Bahrekazari, ‘Player concerns about MMORPG monetization’ (Master Thesis, University of Bergen 2023), 42-46 <<https://bora.uib.no/bora-xmlui/bitstream/handle/11250/3072343/DIKULT350---Master-s-Thesis---Arvinn-Bahrekazari.pdf?sequence=1&isAllowed=y>> accessed 9 November 2025.

¹⁷³ Gupta and Sharma (n 125) 170.

¹⁷⁴ *ibid.*

¹⁷⁵ *ibid.*

and current game development practices.¹⁷⁶ This ambiguity pertaining to loot boxes has also been raised in the context of the 2025 Act.¹⁷⁷

However, as clarified in *K.R. Lakshman* (supra),¹⁷⁸ a mere element of chance is insufficient to categorize the game as a ‘game of chance’. In light of the above discussion on non-monetary gambling and gaming addiction, it becomes necessary to revisit the ratio given in *K.R. Lakshman* (supra) which was delivered 29 years ago (as mentioned above, the *Karnataka High Court* in 2022 also highlighted the need to update the understanding of the negative effects of online games from the old traditional model of the internet to the one used in today’s era).¹⁷⁹

In this regard, it was reported in October of 2024, that an objective framework to differentiate between games of skill and chance was developed,¹⁸⁰ which was also to be sent to the Meity for feedback.¹⁸¹ The framework provides for three tests.¹⁸² The first test pertains to “*persistence of skill*”, which seeks to quantitatively determine a player’s skill by evaluating the consistency in the performance of a player over two different periods of time. The test shows that a player with high success rates in one period of time will be able to continue such consistent performance of high success rate in the other period of time as well (and vice versa) in a game of skill.

The second test pertains to “*experience gap*” which seeks - to assess the correlation between the experience of a user and a successful outcome. In a skill-based game, a more experienced player should statistically have more successful outcomes as compared to a lesser experienced player, with presence of such gap being evidence of the dominance of skill as a factor in determining the game’s outcome. The last test pertains to “*exemplary skill*” which seeks to

¹⁷⁶ *ibid.*

¹⁷⁷ Ashish Deep Verma, ‘Skill Vs Chance Redefined? How Online Gaming Act, 2025 Shifts Legal Landscape’ (*LiveLaw.In*, 24 September 2025) <<https://www.livelaw.in/law-firms/law-firm-articles-/online-gaming-act-shifts-in-legal-landscape-skill-vs-chance-redefined-vidhisastras-ashish-deep-verma-law-firm-articles-304985>> accessed 8 October 2025.

¹⁷⁸ *Dr. K.R. Lakshmanan* (n 171).

¹⁷⁹ *All India Gaming Federation* (n 23).

¹⁸⁰ The Hans India, ‘Skill Games Framework by Professor Bimal Roy: India’s First Quantitative Framework for Online Real Money Games Launched’ *The Hans India* (16 October 2024) <<https://www.thehansindia.com/business/skill-games-framework-by-professor-bimal-roy-indias-first-quantitative-framework-for-online-real-money-games-launched-914873>> accessed 24 December 2024.

¹⁸¹ Aryaman Gupta, ‘Games of skill vs Games of chance: Framework looks to clarify difference’ *Business Standard* (15 October 2024) <https://www.business-standard.com/economy/news/games-of-skill-vs-chance-framework-aims-to-clarify-legal-ambiguity-124101400991_1.html> accessed 24 December 2024.

¹⁸² Dr. Bimal Roy, Kirti Singh and Kazim Rizvi, ‘An Objective Framework To Determine Permissible Online Real Money Games’ (Version 1.0, The Dialogue, 2024), 11-13 <<https://thedialogue.co/wp-content/uploads/2024/10/Digital-Copy-An-Objective-Framework-to-Determine-Permissible-Online-Real-Money-Games.pdf>> accessed 1 October 2025.

assess the exceptional skill shown by certain players when assessed in a spectrum of skill sets, with such players consistently achieving outstanding results.

While this framework is important for understanding the difference between games of skill and chance, it encounters certain problems in the context of *MMORPG* games. The framework has been tested on only three kinds of games, i.e., ludo, poker and fantasy sports¹⁸³ but does not test it on game mechanics (like ‘drop rates’) present in other kinds of more complex and dynamic gameplay formats like fantasy games, including *MMORPG* format games (as mentioned above, the ‘boss fights’ in *MMORPG* games, as per the existing jurisprudence in India would be categorized as games of skill), as well as other kinds of addictive game design. Another issue is that, in applying the tests, it has been mentioned that the outcome of a game should not be determined by chance,¹⁸⁴ which in the case of drop rates in *MMORPG* boss fights would be the case.

IV. CONCLUSION

This paper examined the complex nature of online games in the present era which makes their regulation difficult. Owing to this complexity, regulations have to be framed and interpreted in a dynamic manner to achieve the objective behind such regulations, i.e., to prevent and curb the harms caused by gaming and gambling addiction. To achieve this, regulators must regularly engage with different stakeholders. Furthermore, as regulations evolve to regulate those mechanics previously considered ‘harmless’, the gaming industry must work with other stakeholders to develop alternatives for such mechanics. Also, it is important to ensure that such regulations be interpreted and applied in a consistent manner by the Online Gaming Authority.

In this regard, the key changes derivable from the discussion above and which can be incorporated to more effectively tackle the issue of game design elements involving simulated gambling are:

- (a) Amend the 2025 Act and Rules to explicitly include provisions addressing non-monetary RRM.
- (b) Harmonize the rules applicable to games involving real-world gambling and simulated gambling in relation to advertisement of online games.

¹⁸³ *ibid* 18-22.

¹⁸⁴ *ibid* 16.

- (c) Establish a separate multi-departmental task force which will work in coordination the industry to tackle the issue of real-world trading in online games.
- (d) Establish a research centre dedicated to studying emerging trends in the online gaming sector and its impact on user welfare.

RECONCILING THE DATA-BLIND ARCHITECTURE OF ACCOUNT AGGREGATORS WITH SIGNIFICANT DATA FIDUCIARY OBLIGATIONS UNDER DPDP ACT, 2023

—Shivansh Singh & Devdeep Ahirwal*

ABSTRACT

The Account Aggregator (“AA”) framework in India, designed as a “blind pipe” for financial data flow, is at a crossroads for compliance with the Digital Personal Data Protection (“DPDP”) Act, 2023. This article seeks to highlight this legal deadlock between the RBI’s mandate for the AAs to remain cryptographically blind to the contents of the data to be transferred through them, and the DPDP Act’s de facto imposition of Significant Data Fiduciaries (“SDF”) obligations on AAs, particularly, Data Protection Impact Assessment (“DPIAs”), that mandate access to the aforementioned data to determine “harm”. Moving beyond existing literature that focuses solely on jurisdictional overlap, this article critically analyses the audit paradox, highlighting how the mandated audits under the DPDP Act contravene the RBI’s privacy directive. The article further proposes a metadata-centric safe harbour solution, grounded in the legal frameworks of the United Kingdom and the European Union, to address this lacuna. The article also proposes distinguishing between intermediary fiduciaries and storage fiduciaries and limiting AA’s liability to the consent architecture rather than to the encrypted contents, thereby aligning financial and privacy laws in India without compromising the “Right to Privacy”.

Keywords: Account Aggregators, Data Privacy, Data Privacy Law, Digital Personal Data Protection Act 2023, Intermediary Liability, Reserve Bank of India, Technology Law, Technology Policy, TMT Law.

I. INTRODUCTION

The financial ecosystem in India has undergone a paradigm shift, marking a transformation from a predominantly cash-driven economy to a digitally integrated and data-enabled framework, largely driven by the JAM (Jan Dhan–Aadhaar–Mobile) trinity¹ and the Unified Payments Interface (“UPI”), which recorded a peak of 16.58 billion transactions in October 2024.² Despite this rapid digitisation, the credit market continues to face structural problems, especially in the MSME sector, where a persistent credit gap of ₹20–25 trillion underscores the enduring nature of information asymmetry.³

To resolve this dissonance and support the necessary transformation of credit from ‘asset-based to flow-based,’ the Reserve Bank of India formalised the Account Aggregator system in 2021.⁴ AAs provide a trustworthy third-party platform for digitally transferring the financial details of individuals (such as bank accounts, investments, and insurance) from one financial institution, the Financial Information Provider, to another, the Financial Information User, thereby creating a consent-based ecosystem that gives users control over their data.

As of the end of 2024, such platforms have been successful in providing services for the data-sharing of more than 112 million financial accounts⁵, thus tapping the data capital that was unutilized. Pertinently, the AA architecture operationalises the ‘Right to Privacy’ as upheld by the Hon’ble Supreme Court of India in the case of *Justice K.S. Puttaswamy (Retd.) v Union of India*.⁶ It is embedded in the AA framework by providing consumers with significant control over who can view their financial trail and for how long.⁷ This is technologically enforced

*The author are students at the Integrated Law Course, Faculty of Law, University of Delhi

¹ Ministry of Road Transport & Highways, ‘JAM (Jan Dhan, Aadhar, Mobile) Trinity and Digital Revolution: A Decade of Financial Inclusion, Transparency and Corruption Free India’ (Press Release, 20 December 2024) <<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2086611®=3&lang=2>> accessed 17 January 2026.

² Ministry of Finance, ‘UPI: Revolutionizing Digital Payments in India’ (Press Release, 1 December 2024) <<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2079544®=3&lang=2>> accessed 17 January 2026.

³ Expert Committee on Micro, Small and Medium Enterprises, *Report of the Expert Committee on Micro, Small and Medium Enterprises* (Reserve Bank of India 2019) 59 <<https://dcmsme.gov.in/Report%20of%20Expert%20Committee%20on%20MSMEs%20-%20The%20U%20K%20Sinha%20Committee%20constitutes%20by%20RBI.pdf>> accessed 17 January 2026.

⁴ Ministry of Finance, ‘Celebrating Four Years of Launch of the Account Aggregator Ecosystem - India’s Digital Public Infrastructure (DPI)’ (Press Release, 2 September 2025) <<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2162953®=3&lang=2>> accessed 17 January 2026.

⁵ Sahamati, *Annual Report 2024* (Sahamati 2024) <<https://sahamati.org.in/wp-content/uploads/2024/12/Sahamati-Annual-Report-2024.pdf>> accessed 17 January 2026.

⁶ *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

⁷ AMLEGALS, ‘Deep Dive into India’s Account Aggregator Framework: Consent Architecture, Data Fiduciaries, and Legal Safeguards’ (AMLEGALS) <<https://amlegals.com/deep-dive-into-indias-account-aggregator-framework-consent-architecture-data-fiduciaries-and-legal-safeguards/>> accessed 17 January 2026.

through blind pipe by ensuring that while the user's data is portable, it is also cryptographically isolated even from the intermediary, facilitating its transfer.

Therefore, under the stringent licensing rules set by the RBI, an AA acts as a data courier, with limited access to view, store, or process the financial data it transports.⁸

However, the enactment of the Digital Personal Data Protection Act, 2023 has created a legislative contradiction to the AA model.⁹ By virtue of the sheer volume and sensitivity of the data they facilitate, AA qualify the classification of Significant Data Fiduciaries under *Section 10* of the DPDP Act.¹⁰ This classification imposes an onerous requirement, *viz*, the need to conduct a Data Protection Impact Assessment to audit processing risks, which *ipso facto* presume that the fiduciary undertaking the Assessment has visibility into the content of the said data.¹¹

Consequently, this creates a pivotal compliance paradox at the interface between the two laws. Whilst the RBI mandates the AA to be blind to the data they intercept, the DPDP Act requires them to assess the risk associated with the data they are legally curtailed from decrypting in the first place. Therefore, this article examines how applying common SDF requirements to AA would lead to an inharmony, either by flouting the encryption regime to make the data accessible to AA or by flouting the audit regime to make it, in a sense, private.

This article proceeds in a structured manner to unpack the doctrinal and technical elements of this paradox. The article first defines the essential features of the 'data-blind' mandate of the RBI, demonstrating how regulatory design and cryptographic architecture render the AA incapable of accessing user data. Subsequently, the classification of AA under the DPDP Act is analysed, demonstrating the fundamental mismatch that arises from their inclusion within the ambit of SDF. This conflict is further underscored by examining the audit and compliance requirements under the DPDP Act, in which the obligation to conduct an audit coexists with the structural impossibility of doing so without access to the underlying data. The penultimate section places the Indian position within a comparative context by examining intermediary liability frameworks in the United Kingdom and the European Union, highlighting how these jurisdictions align legal responsibility with data visibility. Finally, a metadata-centric safe harbour framework is mooted in the paper's concluding section, distinguishing between

⁸ Reserve Bank of India, *Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016* (RBI/DNBR/2016-17/45).

⁹ The Digital Personal Data Protection Act, 2023 (22 of 2023).

¹⁰ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 10.

¹¹ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 10(2)(c)(i).

intermediary and storage fiduciaries and offering a doctrinally coherent pathway to reconcile the competing imperatives of privacy, innovation, and regulatory accountability.

II. THE LEGAL TECHNICALITY OF ‘DATA BLIND’ MANDATE

The AA system’s operational infrastructure is based on the tenet of *privacy by design*, under which the intermediary’s blindness to the data is not only incidental but mandatory under a statutory fiat.¹² The data-blind character of the intermediary is ensured through a two-tiered system that combines regulatory restrictions and cryptographic hurdles, which are as follows:

A. The Statutory Prohibition

The RBI (Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016) (“**Master Directions**”) serves as the foundational legal basis for rendering AA data-blind. The Master Directions, *paragraph 6.1*, provides, “*no financial information of the customer shall be retrieved, shared or transferred by the Account Aggregator without the explicit consent of the customer*”¹³ effectively implying that the financial information of the customer accessed by the AA from the FIP can’t reside with the AA, who is bound to transmit the same, thereby acting as a mere courier intermediary of the data and not the custodian itself.¹⁴ This provision creates the legal fiction where the AA merely fetches the data without actually acquiring it.

The provision, therefore, takes away the AA’s right to retain and view the financial data provided by customers. In this limited sense, the AA framework is structurally akin to the mere conduit principle under *Section 79* of the Information Technology Act, 2000, insofar as both regimes limit an intermediary’s interaction with underlying content.¹⁵ However, it is important to highlight that the purpose of invoking *Section 79* is limited to drawing a comparison to highlight its architectural similarity with the AA’s role, limiting the intermediary’s engagement with content rather than being directly applicable as a matter of law.

B. The Cryptographic Enforcement

¹² Leena Datwani and Anand Raman, ‘India’s New Approach to Personal Data-Sharing’ (Working Paper, CGAP 2020) <<https://www.rfilc.org/wp-content/uploads/2021/01/Indias-New-Approach-to-Personal-Data-Sharing.pdf>> accessed 17 January 2026.

¹³ Reserve Bank of India, *Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016* (RBI/DNBR/2016-17/45) para 6(1).

¹⁴ Derryl D’Silva and others, ‘The Design of Digital Financial Infrastructure: Lessons from India’ (2019) BIS Papers No 106.

¹⁵ The Information Technology Act, 2000 (21 of 2000) s 79.

This regulatory requirement is made possible by the Application Programming Interface (API) standardisation specified by Reserve Bank Information Technology Pvt. Ltd. (“ReBIT”).¹⁶ The ReBIT Master Direction provide for the requirement for an end-to-end-encrypted structure.¹⁷ In this process, the FIP encrypts the requested data using a public key generated by the FIU. The AA acts as a simple transport layer for this encrypted message.¹⁸ Importantly, the AA neither possesses the private key nor do they have regulatory approval to demand it.¹⁹ Consequently, the AA operates analogously to a digital messenger tasked with delivering a sealed diplomatic pouch, verifying the consent (the Consent Artefact) for delivery, but never capable of examining the contents (the Financial Data).²⁰ It is this absolute separation of consent flow from data flow that defines the technical environment of the AA regime, which appears to contradict the DPDP Act’s “harm assessment” provisions.

III. LEGAL PARADOX OF FIDUCIARY DUTIES VS. ARCHITECTURAL CONSTRAINTS

The RBI’s architectural mandate and the DPDP Act create a fundamental legal paradox: the RBI framework positions the AA as merely a facilitative infrastructure provider, as discussed in the previous section, whereas the DPDP Act imposes on the AA the responsibility for an active SDF, which shall be undertaken henceforth.²¹ This section, demonstrates that strict compliance with SDF obligations by an AA is operationally impossible without breaching the core privacy premises of the AA license.

The SDF framework delineated under *Section 10(1)* of the DPDP Act empowers the Central Government to notify any data fiduciary as an SDF based on factors, including “*the volume and sensitivity of personal data processed*”.²² AAs, on the other hand, by design, facilitate the

¹⁶ Reserve Bank of India, *Technical Specifications for all Participants of the Account Aggregator (AA) Ecosystem* (RBI/2019-20/96) <<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11729&Mode=0>> accessed 17 January 2026.

¹⁷ ReBIT, *Account Aggregator Ecosystem Master Specifications* (ReBIT 2019) <<https://api.rebit.org.in/schema>> accessed 17 January 2026.

¹⁸ B Jaipal Reddy and B Shirisha Reddy, ‘The Silent Risks of Fin-Tech: Unveiling India’s Regulatory Blind Spots’ in T Ahmad and others (eds), *Proceedings of the International Conference on Law and Technology (ICLT 2025)* (Advances in Social Science, Education and Humanities Research, vol 986, Atlantis Press 2025).

¹⁹ Aditya Sushant Jain, ‘Decoding Consent Managers under the Digital Personal Data Protection Act, 2023: Empowerment Architecture, Business Models and Incentive Alignment’ (2025) 7(4) *Journal of Data Protection & Privacy* 406.

²⁰ Prashant Goyal and others, ‘A Developmental Study to Create Use Cases to Address the Financial and Other Relevant Issues Faced by Millennials through Account Aggregation’ (2024) 33(4) *International Journal of Business Innovation and Research* 506.

²¹ Amit Kumar Kashyap, ‘Rethinking FinTech Regulation under the Indian Data Protection Framework’ (2024) 14(3) *Juridical Tribune-Review of Comparative and International Law* 363.

²² The Digital Personal Data Protection Act, 2023 (22 of 2023) s 10(1)(a).

flow of high-volume (millions of concurrent requests)²³ and high-sensitivity (financial solvency, credit history)²⁴ data, and hence squarely fall within the legal ambit of the SDF classification.²⁵

While it may be argued that AAs primarily operate as Consent Managers, defined under *Section 2(g)*²⁶ rather than traditional Data Fiduciaries defined under *Section 2(i)*²⁷ thereby escaping the SDF liability, the DPDP Act does not explicitly exempt Consent Managers from the SDF classification under *Section 10*, since an extremely high frequency of Data Principals served by the AAs, coupled with the systemic risk they pose to the financial ecosystem, makes the AA's SDF classification imminent and even *de facto*. Moreover, *Section 2(i) of the DPDP Act* establishes “*processing of the personal data*” as the essential ingredient to identify the Data Fiduciary. However, the ‘Processing’ of personal data is defined expansively under *Section 2(x)* to include “*disclosure by transmission*”.²⁸ Thus, by operationalising the retrieval and transmission of financial data and determining the technicality of data flow, AAs satisfy the statutory criteria for a Data Fiduciary. This has also been substantiated by *Entry 8, Part B, First Schedule* of the Digital Personal Data Protection Rules, 2025,²⁹ which levies a fiduciary duty upon Consent Managers in relation to the data principals, with the Consent Manager's qualifications running simultaneously to the AA framework.³⁰

The legislative intent behind the concept of “fiduciary” under the DPDP Act (one who holds data in trust) presumes a degree of custody and visibility which the AA framework explicitly prohibits.³¹ This understanding is consistent with established principles of Indian trust law, wherein fiduciary relationships are founded on the entrustment of property including

²³ Cyril Amarchand Mangaldas, ‘Client Alert: Digital Personal Data Protection Rules 2025’ (January 2025) <<https://www.cyrilshroff.com/wp-content/uploads/2025/01/Client-Alert-DP-Rules-2025-1.pdf>> accessed 12 January 2026.

²⁴ Khaitan & Co, ‘ERGO: Digital Personal Data Protection Rules’ (15 November 2025) <<https://www.khaitanco.com/sites/default/files/2025-11/ERGO%20-%20Digital%20Personal%20Data%20Protection%20Rules%20-%2015%20November%202025.pdf>> accessed 17 January 2026.

²⁵ Sahamati, ‘Reconciling the Account Aggregator and Consent Manager Frameworks’ (*Sahamati Blog*, 18 March 2025) <<https://sahamati.org.in/reconciling-the-account-aggregator-and-consent-manager-frameworks/>> accessed 17 January 2026.

²⁶ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 2(g).

²⁷ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 2(i).

²⁸ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 2(x).

²⁹ Shardul Amarchand Mangaldas & Co, ‘Enforcement of the DPDP Act and Notification of the DPDP Rules’ (21 November 2025) <<https://www.amsshardul.com/insight/enforcement-of-the-dpdp-act-and-notification-of-the-dpdp-rules/>> accessed 17 January 2026.

³⁰ The Digital Personal Data Protection Rules 2025, sch 1 pt B entry 8.

³¹ Ankit Kapoor, ‘Operationalizing Privacy by Design: An Indian Illustration’ (2023) 20(1) SCRIPTed <<https://script-ed.org/article/operationalizing-privacyby-design-an-indian-illustration/>> accessed on 20 December 2025.

information (*Section 3* of the Indian Trusts Act, 1882)³², along with the fiduciary's ability to exercise knowledge, discretion, and control over it for the benefit of another party (*Section 88* of the Indian Trusts Act, 1882)³³. The duties of loyalty, care and accountability that define fiduciary status are thus inherently connected to the fiduciary's ability to access and meaningfully interact with the subject matter of the trust. The SC in the case of *CBSE v Aditya Bandopadhyay* had observed that "... the term fiduciary connotes when one person assumes control and responsibility over another and if the beneficiary has entrusted anything to the fiduciary, to hold the thing in trust or to execute certain acts in regard to or with reference to the entrusted thing, the fiduciary has to act in confidence and expected not to disclose the thing or information to any third party."³⁴

Therefore, without access or custody, which structurally defines the AA's role, fiduciary obligations risk becoming conceptually incoherent

This effectively creates a classification loophole in which AAs are encumbered with the highest degree of compliance obligations whilst having the least permissibility to access the data required for those obligations. This is most evident through the requirement imposed by *Section 10(2)(c)(i)* of the DPDP Act that makes it compulsory for every SDF to perform periodic DPIA³⁵, which by definition, is a tool of risk management intended to assess the "purpose" and "nature" of data to be processed to mitigate any prospective harm to the data principal.³⁶

Harm, in the context of financial data, is inextricably linked to the content of the information.³⁷ For example, leakage of a generic transaction log is less harmful than the leakage of a default notice or a medical insurance payment. Hence, to perform a meaningful DPIA, an AA would need to assess the sensitivity of the data packet to determine the probability and severity of harm.³⁸ Yet, the data-blind prerequisite makes it impossible for the AA to distinguish a benign, low-value transaction from a sensitive, high-value disclosure.

The law, as it stands, requires an assessment of risk in a black box, which posits that the AA must choose between providing a vacuous, blind DPIA or decrypting the data to assess its risk, both of which violate the spirit of the DPDP Act or the RBI Directions, respectively.

³² The Indian Trusts Act, 1882 (2 of 1882) s 3.

³³ The Indian Trusts Act, 1882 (2 of 1882) s 88.

³⁴ *CBSE v Aditya Bandopadhyay* 2011 (8) SCC 497.

³⁵ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 10(2)(c)(i).

³⁶ Ali Alibeigi, 'Bridging the Gap: Assessing India's Digital Personal Data Protection Act in Light of the EU GDPR' (2025) 6(7) SN Computer Science 855.

³⁷ Jaecung Lee and others, 'Investigating Perceptions about Risk of Data Breaches in Financial Institutions: A Routine Activity-Approach' (2022) 121 Computers & Security 102832.

³⁸ Information Commissioner's Office, 'Data Protection Impact Assessments (DPIAs)' (Guidance, 2018) <<https://www.pdpjournals.com/docs/887901.pdf>> accessed 17 January 2026.

Consequently, the DPDP Act's imposition of assessment liabilities on AAs (when treated as SDFs) is particularly problematic, as it overlooks the cryptographic reality of the ecosystem. *Section 8(5)* of the DPDP Act provides that “a data fiduciary must protect personal data in its possession or control”.³⁹ In instances where a data breach is caused by a vulnerability in the encryption standard adopted by the FIP, *Section 33* of the DPDP Act may hold the AA liable for a failure of security safeguards they neither designed nor can verify, since the security framework's vitality is the sole responsibility of FIP.⁴⁰ This, in turn, subjects the courier, i.e., AA, to a strict liability standard in respect of the quality of the sealed envelope, i.e., the encrypted data in this case, on a standard inconsistent with the principle of proportionality.

IV. THE COMPLIANCE ‘CATCH 22’

The AA paradox is further aggravated by the requirement of mandated audits for SDFs. Under *Section 10(2)(b)* of the DPDP Act, it is mandated that each SDF must appoint an Independent Data Auditor to make evaluations regarding compliance with the DPDP Act.⁴¹ Though well-intentioned in promoting compliance, this creates a compliance Catch-22, as again, a mere inspection of the flow to detect compliance requires interference with the compliance structure. One of the main purposes of the data audit is to verify compliance with the “purpose limitation” under *Section 7(a)* of the DPDP Act, which requires that personal data be processed for the stated purpose, i.e., “for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data”.⁴² This could, for instance, involve an audit of transaction records to ensure that data for credit customers was not used for unauthorised marketing purposes, which requires substantive probing of the data. However, in the AA model, “purpose” is encapsulated in the encrypted consent artefact.⁴³ To verify that the actual data packet complies with the consent parameters, the auditor will typically require access to the data in its decrypted form. This will turn the blind pipe into an open and accessible framework, thereby overriding the data-blind requirement under RBI directions.

³⁹ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 8 (5).

⁴⁰ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 33.

⁴¹ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 10 (2) (b).

⁴² The Digital Personal Data Protection Act, 2023 (22 of 2023) s 7 (a).

⁴³ Reserve Bank of India, *Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016* (RBI/DNBR/2016-17/45) para 6.3(iv).

Additionally, the mandated content-level audit introduces a new avenue of vulnerability. In the existing paradigm, the AA ecosystem derives security from the lack of readable data in the AAs' possession, making them unattractive targets for hackers.⁴⁴ However, by being compelled to decrypt their data streams to satisfy their Independent Data Auditor, AAs transform into a hotspot for cyberattacks due to the apparent vulnerability of their operational infrastructure, which would destroy this immunity by design. This is another aspect that would require legislative intervention to avoid any malicious outcome if the SDF classification of AAs is enforced.

A scheme to decrypt private financial information on a systematic scale without a particular accusation of improper conduct directly resembles “an unreasonable search and seizure” prohibited by the SC in *District Registrar & Collector v Canara Bank*.⁴⁵ Hence, any literal enforcement of the DPDP Act obligations on AAs under this interpretation not only introduces a technical problem but also generates a constitutional wrong.

V. GLOBAL PERSPECTIVES: COMPARATIVE APPROACHES TO INTERMEDIARY LIABILITY

To contextualise the Indian inconsistency, it is useful to examine how the interplay of data flow with data visibility is addressed in other global jurisdictions. A comparative analysis between the United Kingdom (UK) and the European Union (EU) suggests that India's statutory insistence on a “blind pipe” architecture is unique in creating a liability vacuum inapplicable in regimes where aggregators act as transparent data processors. The need to undertake such a comparative analysis becomes necessary to dissect the regulatory blind spot and dissonance in India's nascent data protection regime. Analysing the foreign jurisdiction, specifically the UK and the EU, allows us to highlight the architectural anomaly in India's regime in a constructive manner, while providing a functional model of harmonisation between the legal incongruity highlighted in the Indian context.

A. The UK: Open Banking and the ‘Root Cause’ Liability

The UK's Open Banking framework, regulated by the Competition and Markets Authority (CMA) and the Financial Conduct Authority (FCA), is based on a very different liability model.

⁴⁴ *ibid.*

⁴⁵ *District Registrar & Collector v Canara Bank* 2005 (1) SCC 496.

Under the Payment Services Regulations 2017 (PSRs), Third Party Providers (TPPs) (the UK equivalent of AAs) are not data blind.⁴⁶ They can access, store, and analyse customer data⁴⁷ in order to offer value-added services (e.g., budgeting tools).⁴⁸

Since TPPs have visibility into the data, the law logically holds them liable for its security. The UK ecosystem addresses the liability question by employing a “root cause” mechanism, whereby, in the event of a data breach, the regulator traces the unencrypted data to the point of breach, and liability rests there.⁴⁹ This creates perfect symmetry, with the liability following the breach.

Moreover, the UK framework prescribes “traceability” in no unclear terms for the prevention of financial crime. The Joint Money Laundering Steering Group guidelines impose an obligation on the intermediary to retain sufficient data to reconstruct transactions for audit trails.⁵⁰ This, in effect, makes it impossible to adopt a zero-knowledge architecture as prescribed by the RBI in the Indian regime.

Therefore, UK TPPs are never required to perform any risk assessment on data they cannot see, given that their compliance requirements are fully aligned with their technical access.

B. The European Union: PSD2 and the ‘Data Controller’ Clarity

In the EU, the Second Payment Services Directive (PSD2) regulates Account Information Service Providers (AISPs).⁵¹ Unlike the AAs in India, which act as data routes, EU AISPs are classified under the General Data Protection Regulation (GDPR) as “Data Controllers”.⁵² An AISP is an active processor that aggregates and enriches data for the user. Since they determine the means and purposes of processing, the GDPR rightfully imposes heavy impact assessment obligations, or DPIAs, on them.⁵³

However, the EU provides a legislative safety valve that is notably absent in the Indian framework – for intermediaries that act purely as conduits of transmission, the Digital Services Act provides a mere conduit exemption under *Article 4*.⁵⁴ This shields the intermediary from

⁴⁶ Payment Services Regulations 2017, SI 2017/752.

⁴⁷ Payment Services Regulations 2017, reg 70.

⁴⁸ Payment Services Regulations 2017, reg 97.

⁴⁹ Payment Services Regulations 2017, reg 95.

⁵⁰ Han-Wei Liu, ‘Shifting Contour of Data Sharing in Financial Market and Regulatory Responses: The UK and Australian Models’ (2021) 10 American University Business Law Review 287.

⁵¹ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market [2015] OJ L337/35, art 33.

⁵² European Data Protection Board, *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR* (Version 2.0, EDPB 2020).

⁵³ *ibid.*

⁵⁴ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1, art 4.

any liability for the information transmitted, provided the intermediary does not interfere with the content.

The EU's legal framework thus allows for two distinct classes, *viz*, the Active Processor, which is fully liable, and the Passive Conduit, which is exempt.⁵⁵ India's DPDP Act does not make such a distinction for AAs and thus forces the passive conduit, that is, the AA, to bear the full brunt of a law meant for an active processor, that is, the AISP.

C. Lesson for India's Data Protection Regime vis-à-vis Global Framework

A synthesis of these comparative frameworks reveals a consistent regulatory logic, i.e., responsibility is determined by the degree of data visibility and control exercised by the intermediary. Both the UK and the EU reserve increased fiduciary and audit responsibilities for actors that determine the goals and methods of processing, while avoiding imposing compliance obligations on organisations that do not have meaningful access to the underlying data. The Indian framework under the DPDP Act, in contrast, lacks such calibration by integrating a zero-knowledge architectural mandate with the full spectrum of fiduciary obligations. The very compliance dilemma noted in this article is thus created by the lack of a clear doctrinal demarcation between active processors and passive conduits, underscoring the need for a tailored regulatory strategy that balances legal obligations with technical capabilities.

VI. RECOMMENDATION: 'METADATA-CENTRIC' SAFE HARBOUR

To break this impasse between the privacy-protection architecture provided by RBI and the risk-reduction mandates under the DPDP Act, it is necessary to adopt a more nuanced regulatory regime that cannot be defined by a one-size-fits-all rubric for fiduciary duty. To resolve this, a "Metadata-Centric Safe Harbour Regime" for AAs can be conceived, which would be legally anchored in the distinct operational nature of "Intermediary SDFs" versus "Storage SDFs".

This article posits a three-pronged regulatory approach to operationalise this regime. Firstly, the article recommends separate, clear legal definitions that distinguish storage and intermediary fiduciaries. Secondly, it recommends replacing content-level assessments with cryptographic metadata audits, and thirdly, it provides a conditional safe harbour for AAs, protecting them from content-related liability. These recommendations propose protections that

⁵⁵ Giancarlo Frosio, 'The Death of "No General Monitoring Obligation"? A Pulse Check on the DSA' (2023) 14(2) *Journal of Intellectual Property, Information Technology and E-Commerce Law* 123.

enable compliance systems to validate data flow integrity without compromising the encryption of transmitted data.

A. Differentiating Fiduciary Classes

The Data Protection Board (DPB) can utilise its powers under *Section 28(1)* of the DPDP Act to issue a guidance note⁵⁶ that would define “processing” with respect to AAs to explicitly clarify that, while AAs are SDFs by volume, their fiduciary duty is limited only to the integrity of the facilitation framework of the encrypted data, and not the substantive safety of the data being transferred. This would enable a two-tier system of compliance, i.e., storage SDFs (Banks/FIPs) would be liable for data content risks, while intermediary SDFs, such as AAs, would be solely liable for risks associated with the consent architecture.⁵⁷

B. The Mechanism: The Metadata Audit

Consequently, the auditing and DPIA obligations in *Section 10 of the DPDP Act* can be reinterpreted in the context of AAs to focus exclusively on Metadata Compliance.⁵⁸ This means that, instead of assessing the encrypted payload, the scope for the Independent Data Auditor’s audit will check the consent artefact. The audit will therefore examine the facilitative and architectural aspects of the data framework, including inquiries such as whether the consent was valid, whether the timestamp was valid for the actual fetch request, whether the encryption algorithm used was in accordance with ReBIT standards, etc.

Based on the judicial principles of *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*⁵⁹, the compliance can be established by electronic certificates under *Section 65B* of the Indian Evidence Act, 1872⁶⁰, thereby confirming the integrity of the transaction logs and the hash value of the data packet. Where the hash value is the same on both the FIP and FIU sides, the AA will fulfil its fiduciary obligation.

This will thus be duly adjudicated as a cryptographic audit, fully compliant with the DPDP Act in respect of transparency, thereby harmonising the requirement to decrypt with the RBI’s prohibition.

⁵⁶ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 28(1).

⁵⁷ Malavika Raghavan and Anubhuti Singh, ‘Regulation of Information Flows as Central Bank Functions? Implications from the Treatment of Account Aggregators in India’ (2020) Center on Finance, Law & Policy Working Paper <<https://financelawpolicy.umich.edu/sites/cflp/files/2021-10/raghavan-singh-regulation-of-information-flows-as-central-bank-functions-implications-from-treatment-account-aggregators-india.pdf>> accessed 17 January 2026.

⁵⁸ *ibid.*

⁵⁹ *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

⁶⁰ The Indian Evidence Act, 1872 (1 of 1872) s 65B; The Bharatiya Sakshya Adhiniyam, 2023 (47 of 2023) s 63(4).

C. The Safe Harbour Provision

Additionally, the Central Government can notify exemptions for AAs under *Section 17(3)*⁶¹ or further clarify in the rules that AAs are exempt from the law on content harm. This would effectively allow any malicious software communication packet that damages the principal to shift the blame to the FIP (sender) or the FIU (decryptor). The AAs can also be granted a safe harbour contingent on their maintaining the blind pipe architecture. This would ensure that the law does not punish but rather promotes the development of the very same encryption tools that ensure the anonymity of Internet users.

VII. CONCLUSION

The AA system brings about a paradigm shift in India's digital economy, from a model of data hoarding to one of data democratisation. The current tension, however, arises between the RBI's data-blind mandate and the DPDP Act's fiduciary obligations, which may undermine the newfound momentum if not resolved. Therefore, this article highlights this ostensible shift in the mandate of the AAs moving from the role of a blind intermediary facilitator to that of a content-aware guardian, which requires satisfaction of one law at the expense of the other. Pursuant to this, the article demonstrates that the way out accordingly does not lie in stripping the system of the current and necessary layer of encryption, but in making the scales of compliance responsive to the unique character of the AA system.

This article moves beyond a theoretical critique of the current regulatory stalemate and offers a concrete three-pronged legislative scheme. First, it lays down the imperative to separate Intermediary Fiduciaries from Storage Fiduciaries, such that liability is based on where the fiduciary has operational control over the data, rather than merely on where the data is flowing. Second, it provides a practical modality to maintain this separation by replacing the invasive DPIAs with mathematically verifiable Cryptographic Metadata Audits. Finally, this article proposes a statutory safe harbour provision that immunises AAs from liability for the content they provide to consumers, so long as they comply with the blind pipe' architecture.

However, it is also important to understand the limitations of the recommendations mentioned above. A metadata-centric audit is only effective when the cryptographic consent is intact and therefore does not remedy vulnerabilities associated with false consent forms created to obtain consent or with tampering with metadata before it is sent. To address these shortcomings, additional legislation introspection needs to be enacted, along with technical sandboxing, to

⁶¹ The Digital Personal Data Protection Act, 2023 (22 of 2023) s 17(3).

create a safe harbour fortified against high-end consent-layer fraud, without reverting to content-level monitoring.

Given the immediate⁶² and narrow compliance window for regulatory intervention,⁶³ the article provides grounds for the Data Protection Board and the Ministry of Electronics and Information Technology (MeitY) to legislate to address this gap in forthcoming guidance under the DPDP Rules. The new approach, hence, ought to be centred on the metadata of the encryption, which would allow the Indian financial and privacy frameworks to align with each other, ensuring that the ‘Right to Privacy’ does not block the ‘Right to Credit’.

⁶² The Digital Personal Data Protection Rules 2025, r 1.

⁶³ Shardul Amarchand Mangaldas & Co, ‘Enforcement of the DPDP Act and Notification of the DPDP Rules’ (21 November 2025) <<https://www.amsshardul.com/insight/enforcement-of-the-dpdp-act-and-notification-of-the-dpdp-rules/>> accessed 17 January 2026.

ALTERNATE APPROACHES TO AI PERSONHOOD: ACCOMMODATING A NEW JURISPRUDENTIAL CHALLENGE

—Prerana Srinath*

ABSTRACT

With the advent of the post-ChatGPT era of artificial intelligence, scholarly discourse on extending legal personhood to AI systems has gained renewed momentum. Scholars have moved a step further from the question of whether there is a need to recognize AI as an individual legal person and have shifted their focus to exploring how AI's personhood can be accommodated within existing legal structure. This line of scholarship, which is situated in the intersection of technology law and company law, also finds resonance in environmental law jurisprudence where courts have toyed with the idea and implications of recognizing natural resources like rivers and lakes as legal persons vested with varying degrees of rights. While courts in other jurisdictions such have limited themselves to recognizing only rights specific to nature, such as the right to exist and right to regenerate, Indian courts have pushed the margins and grappled with the possibility of assigning full legal personhood to such non-sentient entities.¹ This is precisely what makes the Indian judgments pivotal to understanding how the jurisprudence on recognition of legal personhood of AI could pan out in the future and this will be the enquiry that this paper embarks on. In undertaking this research, I will be adopting a qualitative case study-based methodology, and the analysis will engage with the question of whether the rationale used by Indian courts in cases pertaining to legal personhood of lakes and rivers etc., can be abstracted sufficiently to also apply to Artificial Intelligence.

Keywords: *Artificial Intelligence; AI Regulation; Personhood theory, Corporate personality; Environmental law.*

* The author is a student at O.P. Jindal Global University, Jindal Global Law School.

¹ Mihnea Tanasescu, 'When a river has the status of a person: From New Zealand to India, Nature Gets its Day in Court' (*Scroll.in*, 20 June 2017) <<https://scroll.in/article/841103/when-a-river-has-the-status-of-a-person-from-new-zealand-to-india-nature-gets-its-day-in-court>> accessed 09 April 2026.

I. INTRODUCTION

When Isaac Asimov first wrote about robots as conscious and autonomous beings and laid down the now famous three laws of robotics in his 1942 short story ‘Runaround’,² the interest around the possibility of actually creating a self-thinking machine which could fool people into believing that it is a real human had just been ignited by scientists like Alan Turing.³ Fast forward seventy years, and we are now much closer to that goal of creating self-thinking autonomous machines than ever,⁴⁵ and accompanying this technological optimism has been a growing concern about how the law can be recast to assimilate and account for these developments.⁶⁷ One specific piece of this legal puzzle that has elicited much interest,⁸ has been the question of whether it is, or would be in expectant future, necessary to grant legal personhood,⁹ to such autonomous, artificially intelligent machines,¹⁰¹¹ and, if so, whether the existing legal framework would be malleable enough to bring about this change in jurisprudence.¹²¹³

The present article attempts to embark upon an enquiry of the latter question by considering alternate ways through which the personhood of AI systems could be accommodated within

² Isaac Asimov, ‘Runaround’ in *I, Robot* (Doubleday 1950).

³ BJ Copeland, ‘History of Artificial Intelligence’ (*Encyclopædia Britannica*, 26 March 2024) <<https://www.britannica.com/science/history-of-artificial-intelligence>> accessed 27 April 2025.

⁴ J Zhou, P Ke, X Qiu, M Huang and J Zhang, ‘ChatGPT: Potential, Prospects, and Limitations’ (2023) *Frontiers of Information Technology & Electronic Engineering* <<https://doi.org/10.1631/FITEE.2300089>> accessed 27 April 2025.

⁵ S Bubeck and others, ‘Sparks of Artificial General Intelligence: Early Experiments with GPT-4’ (2023) *arXiv preprint arXiv:2303.12712* <<https://arxiv.org/abs/2303.12712>> accessed 27 April 2025.

⁶ Amlan Mohanty and Shatakrtu Sahu, ‘India’s Advance on AI Regulation’ (*Carnegie Endowment for International Peace*, 21 November 2024) <<https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en¢er=india>> accessed 27 April 2025.

⁷ Bill Whyman, ‘AI Regulation Is Coming: What Is the Likely Outcome’ (*Center for Strategic and International Studies*, 10 October 2023) <<https://www.csis.org/blogs/strategic-technologies-blog/ai-regulation-coming-what-likely-outcome>> accessed 27 April 2025.

⁸ Visa AJ Kurki and T Pietrzykowski, ‘Introduction’ in *Legal Personhood: Animals, Artificial Intelligence and the Unborn*, vol 19 (1st edn, Springer 2017) <<https://doi.org/10.1007/978-3-319-53462-6>> accessed 27 April 2025.

⁹ Jaynes TL, ‘Legal Personhood for Artificial Intelligence: Citizenship as the Exception to the Rule’ (2019) 35 *Journal of Knowledge, Culture and Communication* 343 <<https://philarchive.org/archive/JAYLPF>> accessed 2025.

¹⁰ Karina Parikh, ‘Artificial Intelligence: Should Robots Have Rights?’ (*AVASANT*, 2020) <<https://avasant.com/report/artificial-intelligence-should-robots-have-rights/#:~:text=They%20are%20not%20living%20beings,ability%20to%20work%20more%20efficiently>> accessed 9 April 2026.

¹¹ Abhivardhan, ‘An Indic Approach to Artificial Intelligence and Constitutionalism’ (*RGNUL Student Research Review*, 2020) <<https://www.rsrr.in/post/an-indic-approach-to-artificial-intelligence-and-constitutionalism>> accessed April 2025.

¹² Claudio Novelli, Luciano Floridi, Gunther Teubner and Giovanni Sartor, ‘AI as Legal Persons: Past, Patterns, and Prospects’ (2024) *SSRN Electronic Journal* <<https://dx.doi.org/10.2139/ssrn.5032265>> accessed 2025.

¹³ Hashiguchi M, ‘Constitutional Rights of Artificial Intelligence’ (2024) 19 WASH. J. L. TECH. & ARTS <<https://digitalcommons.law.uw.edu/wjlta/vol19/iss2/2/>> accessed 9 April 2026.

existing legal structures, through focusing on insights drawn from environmental law cases. Accordingly, the article proceeds by first establishing the nexus between environmental law and AI regulation and then reviewing a small number of cases on recognition of legal personhood of environmental entities, to understand how environmental law jurisprudence can enrich our understanding of the potential trajectory for recognition of AI personhood.

II. UNDERSTANDING EVOLUTION OF PERSONHOOD

In simple terms, ‘personhood’ or ‘*legal* personhood’ is the concept through which the law recognizes an entity as being clothed with rights and obligations. And central to such recognition, is the Law’s conception and understanding of *what constitutes a legally recognizable entity*. In other words, in order for the law to designate someone as a person and provide mechanisms for the protection of their rights and enforcement of their obligations, there are certain standards which they must show to meet. These standards define their ability to be *entitled* to those rights and certify their capability to fulfil the attendant duties and obligations. Thus, the legal recognition of personhood at any point of time or in any particular place, is contingent on the prevailing standards, regarding what constitutes a legally recognizable entity, which exist in *that* place and at *that* time.

Early ideas of personhood were extremely exclusionary and even natural persons including slaves under Roman¹⁴ and New Spain’s¹⁵ (modern-day Mexico) laws and African Americans in the US¹⁶ were not given legal recognition. This was a consequence of the norms that prevailed in those times and in those regions, which deemed slaves and African American persons to be of a lower standing. However, with the evolution of time and society, and a wider recognition of concepts such as liberty and equality, the jurisprudence on who the law was willing to accept as legally identifiable persons also came to evolve. The idea of personhood slowly continued to expand so widely that there came a point where a new concept called ‘juristic person’ came to be founded. At the core of the idea of ‘juristic person’ was the creation of a *legal fiction* through which the law would recognize the personhood of even an artificial entity which was otherwise not even a biological person.¹⁷ Under this concept, corporations

¹⁴ Visa A.J. Kurki, ‘A Short History of the Right-Holding Person’ in *A Theory of Legal Personhood* (Oxford, 2019; online edn, Oxford Academic, 19 Sept. 2019).

¹⁵ Brian P Owensby, ‘Legal Personality and the Processes of Slave Liberty in Early-Modern New Spain’, (2009) 16(3) *European Review of History: Revue Européenne d’histoire*, 365–382. <<https://doi.org/10.1080/13507480902916928>> accessed 9 April 2026.

¹⁶ *Dred Scott v Sandford* (1857) 60 US 393.

¹⁷ *Shiromani Gurudwara Prabandhak Committee, Amritsar v Shri Som Nath Dass & others* (2000) 4 SCC 146.

and other enterprises were all deemed to be persons and were all clothed with rights, duties and obligations for the purpose of law.¹⁸

III. CORPORATIONS, ENVIRONMENT AND AI

Considering the above-mentioned history of the evolution of personhood, it might be valid to argue that studying the jurisprudence on how corporations and other human-made entities gained recognition as juristic persons is a valuable resource for analysing the extension of personhood to AI, another comparably non-biological entity. However, the juristic personality of corporations is now¹⁹, as opposed to a century ago, when it was still a contested terrain, a largely settled²⁰ and universally well accepted theory. On the other hand, environmental law jurisprudence in this regard has been more recent and less static. There is much less consensus on whether, how and to what extent natural entities like animals, rivers or trees should be recognized as juristic persons. As such, this line of cases supplies us with more information on the implications of and challenges that we may encounter in giving legal recognition to AI's personhood.

The second ground for referring to environmental jurisprudence as opposed to that of company law is because, even as these corporations have come to be recognized as having an independent legal identity as juristic persons, the *dominant* theories of corporate governance continue to understand a company as represented by its management and directors, as an agent of the shareholders²¹ or stakeholders which takes decisions that either help maximize value for them²² or, more generally, are in their best interest.²³ Over the years, there have been proponents for alternative approaches that advocate for recognising companies as individual natural persons, fully divorced from their association with shareholders, like the 'natural entity' theorists. However, such theories have unfortunately not sustained and have instead been overtaken by defenders of a shareholder-centred vision of corporate personhood, like the 'nexus of contracts' theorists who continue to hold sway in current times.²⁴ Thus, the

¹⁸ *Salomon v Salomon & Co Ltd.* (1896) UKHL 1.

¹⁹ John Dewey, 'The Historic Background of Corporate Legal Personality' (1926) 35 *Yale Law Journal* 655.

²⁰ Patrick John Fitzgerald, *Salmond on Jurisprudence* (12th edn, Sweet & Maxwell 2020) 305.

²¹ *Bumper Development Corp Ltd. v Metropolitan Police Commissioner* (1991) 1 WLR 1362.

²² Sorin Nicolae Borlea and Monica-Violeta Achim, 'Theories of Corporate Governance' *Studia Universitatis "Vasile Goldis" Arad. Seria stiinte economice*. (2013) 117 <<https://www.semanticscholar.org/paper/THEORIES-OF-CORPORATE-GOVERNANCE-Borlea-Violeta/63097f4b12d0768218e499049577aac3859842ec>> accessed 2025.

²³ James A. Stieb, 'Assessing Freeman's Stakeholder Theory' (2009) 87 *Journal of Business Ethics* 401.

²⁴ David Millon, 'Theories of the Corporation' (1990) *Duke Law Journal* 201 <<https://scholarship.law.duke.edu/dlj/vol39/iss2/2>> accessed 9 April 2026.

predominant ideas on corporate personality continue to refrain from fully divorcing the juristic personality of a company from its association with other natural persons, whose interests dictate the manner and direction of the company's functioning.

In contrast, environmental jurisprudence in India has adopted an eco-centric approach, recognizing rivers, lakes, and glaciers as independent entities whose rights are distinct from and equal to those of natural persons. These entities are not regarded as agents *of* shareholders or other human persons (although an agent is nonetheless required to act *on their behalf* for legal *representation* purposes when it comes to suing and being sued). The current state-of-art in technological advancements in AI is at the *threshold* of similarly progressing beyond a point where it can be seen as a mere tool or property in the hands of a natural person.²⁵²⁶ Considering the dynamic nature of this technology and mercurial pace of its evolution, it would not be inconceivable to expect AI to develop to a point where it functions independently of human involvement. Thus, referring to the jurisprudence on environmental entities whose existence is similarly not dependent on or necessarily associated with other natural persons, would be useful in preparing a blueprint for simultaneous evolution of legal regulations to deal with such a scenario.

Finally, in dealing with the questions of fundamental rights of that are vested in corporations, Indian courts²⁷²⁸ have been reluctant to extend all fundamental rights to such companies and corporations. Among various reasons, it has been argued that a company cannot be construed to be a citizen²⁹ and as such, it cannot claim applicability of every right under Article 15, 16 and 19 to their full extent in the way they are otherwise applicable to ordinary humans.³⁰ Contrarily, although the environmental cases are but a few in number, the courts here have explicitly refrained from limiting the various rights that these environmental entities may be entitled to. A textual evaluation of the judgements reveals that the courts have employed expansive terms³¹ and have stated that fundamental rights would be applicable to rivers,

²⁵ S Bubeck and others, 'Sparks of Artificial General Intelligence: Early Experiments with GPT-4' (2023) *arXiv preprint* arXiv:2303.12712 <<https://arxiv.org/abs/2303.12712>> accessed 27 April 2025.

²⁶ Marco Dehnert and David J Gunkel, 'Beyond Ownership: Human–Robot Relationships Between Property and Personhood' (2023) 27 *New Media & Society* 1110 <<https://journals.sagepub.com/doi/abs/10.1177/14614448231189260?mi=ehikzz>> accessed 9 April 2026.

²⁷ *Jupiter General Insurance Co. Ltd. v Rajagopalan* (1952) AIR PUNJAB 9.

²⁸ *Sree Meenakshi Mills Ltd. v State of Madras* (1951) AIR MADRAS 974.

²⁹ David Millon, 'Theories of the Corporation' (1990) *Duke Law Journal* 201 <<https://scholarship.law.duke.edu/dlj/vol39/iss2/2>> accessed 9 April 2026.

³⁰ *State Trading Corporation of India Ltd. v Commissioner* (1974) ILR DELHI 58.

³¹ Katie Surma, 'Indian Court Rules That Nature Has Legal Status on Par with Humans and That Humans Are Required to Protect It' (*Inside Climate News*, 4 May 2022) <<https://insideclimatenews.org/news/04052022/india-rights-of-nature/>> accessed 2025.

glaciers and even mother nature in the same way and to the same extent that they are applicable to humans.³² This is more important for our purposes as, when we talk about the rights of AI, some of the most relevant rights that AI would want to claim protection for would pertain to, among others, Article 19 (rights to freedom, including freedom of expression, freedom of occupation and trade, etc.). For instance, consider the spawning of cases³³³⁴³⁵ pertaining to violation of personality rights by AI. While dealing with such cases, for an AI to be able to claim a free speech exception under Article 19 as a defence, it would have to first be recognized as a citizen.

Having thus established the vitality and resourcefulness of studying these environmental cases, it is necessary to add a caveat that these environmental cases themselves refer substantially to how jurisprudence on rights of corporations came to be recognized as a part of their judicial analysis. To that extent, the aim of this research is *not* to discredit the contribution that a study of legal personhood of corporations can make towards understanding the future possibilities with respect to personhood of AI. Rather, it is simply to explore the subject from the perspective of another set of cases which, owing to its contested acceptance and innovative reasoning employed, provides us with more bandwidth to understand the possible future trajectory of regulating AI personhood.

IV. CASE REVIEW

We now look at a few judgements to understand what the Indian cases on recognizing the legal personhood of non-human, natural entities like lakes and rivers tell us about the possibility of accommodating the legal personhood of AI. The cases mentioned herein were selected on an exhaustive (as on the date of submission of the manuscript) search of judgements dealing specifically with personhood of environmental entities. In conducting this analysis, we will firstly determine the court's definitional understanding of 'juristic personhood' in each case and evaluate what, in the court's perspective, is the legal or non-legal basis for extending personhood to natural, non-human elements. This evaluation is important since, as mentioned earlier, the question of whether an entity can be recognized as a legal person primarily revolves around prevailing norms on what constitutes personhood.³⁶ Thus, using these cases on

³² *Lalit Miglani v State of Uttarakhand* (2017) SCC Online Utt 392.

³³ *Arijit Singh v Codible Ventures LLP* (2024) SCC OnLine Bom 2445.

³⁴ *Global Health Limited and Ors. v John Doe and Ors.* (DEOR 2025) MANU DEOR 2502/2025.

³⁵ *Devi Prasad Shetty v Medicine Me* (2024) SCC OnLine Del 8565.

³⁶ Visa A. J. Kurki, *Legal Personhood* (Cambridge University Press, 2023) <<https://www.cambridge.org/core/elements/legal-personhood/EB28AB0B045936DBDAA1DF2D20E923A0>> accessed 09 April 2026.

environmental jurisprudence, if we are able to construct the Indian judicial system's current conception on what defines legal personhood, we would be better positioned to further deduce whether AI would also fit within the framework of such a conception, in order for it to also be deemed as a legally recognizable entity. Consequently, the second arm of the analysis will focus on understanding whether the non-legal bases which the court has relied on in granting personhood to environmental elements, can also be found to predicate the need or demand for granting legal personhood to AI. Thus, the overall aim of this case study would be to understand whether the non-legal reasons relied on by the courts to grant personhood to environmental entities, can be sufficiently abstracted to make an argument for similarly extending personhood to AI as well.

This evaluation, specifically, of *the non-legal bases or reasons* for the expansion of the personhood, is necessitated upon the understanding that under common law, courts often rely on non-legal bases in their exercise of development of the law. Similarly, even in the evolution of the concept of juristic personhood, courts have invariably relied on non-legal, sociological and philosophical foundations.³⁷ Scholars³⁸ such as John Dewey³⁹ have argued that such reliance on such non-legal bases can be detrimental for rule of law and have instead advocated that the applicability of a strictly legal definition of the concept, should be the basis for extending juristic personhood to any entity. The evaluation of *whether* courts should *at all* ground their definitional understanding of juristic personality in non-legal foundations is beyond the scope of this paper. Considering that courts *do in fact* rely on non-legal foundations, it is necessary for an effective and fair analysis of the cases, to acknowledge these non-legal arguments which form the basis for a legal extension of personhood. In any case, scholars and researchers exploring the intersection of AI and legal personhood have often relied on non-legal, metaphysical and even moral arguments in their work.⁴⁰ Thus, a strict, untraversable distinction between non-legal and legal grounds seems to be of much less consequence here.

³⁷ Peter Birks (ed), *English Private Law* (Vol I, Oxford University Press 2000).

³⁸ Rafael Dean Brown, 'Property Ownership and the Legal Personhood of Artificial Intelligence' (2020) 30 *Information & Communications Technology Law*, 30(2), 208–234, <<https://doi.org/10.1080/13600834.2020.1861714>> accessed 9 April 2026.

³⁹ John Dewey, 'The Historic Background of Corporate Legal Personality' (1926) 35 *Yale Law Journal* 655.

⁴⁰ David J Gunkel, *Person, Thing, Robot: A Moral and Legal Ontology for the 21st Century and Beyond* (Cambridge MA: MIT Press 2023).

*A. Mohd. Salim v State of Uttarakhand (2017)*⁴¹

In this case, the Uttarakhand HC held that the rivers Ganga and Yamuna were legal and juristic entities and assigned them with all corresponding rights, duties and liabilities that are otherwise attached to a natural person.⁴² In coming to this conclusion, it broadly relied on two non-legal arguments. Firstly, it referred to the case of *Ram Jankijee Deities v State of Bihar*⁴³ case where, the religious efficacy of a temple, based on the consecration of an idol which had revealed itself to the people as an image of God, was made the foundation of assigning juristic personality to the idol. That is, the juristic personhood was found to originate out of non-legal, Hindu religious belief and performance of similarly non-legal religious ceremonies. Secondly, the court relied on the case of *Shiromani Gurudwara Prabandhak Committee*⁴⁴ where a sociological argument had been made that the necessity to fulfil social and scientific objectives of human development was the non-legal basis for extending legal personhood. The court applied this argument to note that the juristic personality of an entity was necessary for “sub-serving the needs and faith of the society”. Further, the court legally defined the term ‘juristic person’ as an entity which is capable of bearing rights and duties in furtherance of a legal relationship. It referred to the *Corpus Juris Secundum* to note that a juristic person would be any entity which is so created and devised by human laws for the purpose of society and government.

*B. Lalit Miglani v State of Uttarakhand (2017)*⁴⁵

The petitioners in this case had applied to the Uttarakhand HC shortly after the pronouncement of the judgement in the *Mohd. Salim*⁴⁶ case seeking declaration of the Himalayas, its glaciers and other waterbodies as juristic persons in line with the recognition granted to Ganga and Yamuna in that case. The court held in favour of the applicants and noted that rivers, lakes and other water bodies have an inherent right to not be polluted and more importantly, declared them to be juristic persons with all corresponding rights, duties and liabilities of a living person including fundamental rights which were to be treated at par with the rights of human beings. But the most crucial and relevant aspect of this case was the court’s observation that rivers, lakes, glaciers and other water bodies were scientifically and biologically living entities and

⁴¹ *Mohd. Salim v State of Uttarakhand* (2017) SCC OnLine Utt 367.

⁴² Shyam Divan and Armin Rosencranz, ‘Public Interest Litigation’ in *Environmental Law and Policy in India: Cases and Materials* (3rd edn, Oxford University Press 2022) <<https://doi.org/10.1093/oso/9780192865458.003.0002>> accessed 20 April 2025.

⁴³ *Ram Jankijee Deities v State of Bihar* (1999) 5 SCC 50.

⁴⁴ *Shiromani Gurudwara Prabandhak Committee, Amritsar v Shri Som Nath Dass & others* 2000 (4) SCC 146.

⁴⁵ *Lalit Miglani v State of Uttarakhand* (2017) SCC Online Utt 392.

⁴⁶ *Mohd. Salim v State of Uttarakhand* (2017) SCC OnLine Utt 367.

thus they had a right to exist. Apart from this, the court also called on the sociological reasoning used in the *Mohd. Salim* judgment that the evolution of the concept of juristic person was necessary to meet the needs of social and scientific development. It further defined juristic persons legally as any entity which had been conferred with rights and obligations in law, and non-legally as any entity which “acts like a natural person”.

*C. Court on its own motion v Chandigarh Administration (2020)*⁴⁷

This case dealt with the assignment of juristic personality to the Sukhna lake in Chandigarh. The judgement followed broadly the same line of analysis as was undertaken in the previous two cases. However, in addition to the sociological and strictly legal reasons, the court also noted that it was necessary to accord personhood to the lake in order to able to preserve and protect it and the various living beings within it as well as other natural persons like fishermen and boaters who depended on it for their livelihood. In making this assertion, the court drew from the dissenting judgement written by Justice Douglas in the American case of *Sierra Club v Morton*.⁴⁸

*D. A. Periyakaruppan v State (2022)*⁴⁹

In this case, the matter related to an administrative law issue concerning a Tahsildar who had illegally issued *pattas* to a protected forest area. The court cited the Lalit Miglani⁵⁰ case mentioned above and adopted the language used by the court in that case to declare ‘Mother Nature’ as a legal and juristic person and assigned it with all fundamental, legal and constitutional rights, duties and liabilities that are necessary for its survival and wellbeing in order to preserve the nature.

V. ABSTRACTING THE ARGUMENTS

Having thus delved into each of the few environmental cases, we can broadly note that in defining a juristic person, the court has consistently adopted a legal approach and has noted that a juristic person is *any entity which has either been designated as such by law and legal procedure or has been recognized as being capable of possessing rights and duties by the law*. This technical legal definition is, however, *not* applied in vacuum and the court has concomitantly substantiated it by taking note of the non-legal, religious/ socio-economic

⁴⁷ *Court on its own motion v Chandigarh Administration* (2020) SCC OnLine P&H 4454.

⁴⁸ *Sierra Club v Morton* (1972) Sec. Int. 405 US 727.

⁴⁹ *A. Periyakaruppan v State* (2022) SCC OnLine Mad 2077.

⁵⁰ *Lalit Miglani v State of Uttarakhand* (2017) SCC Online Utt 392.

factors underlying such a designation by the law. So, while the criteria for being classified as a juristic person is assignment of rights and duties, the reason for such assignment can be sociological or religious. Notably, the first three judgements were all delivered by benches involving Justice Rajiv Sharma and although the first two judgements were subsequently stayed by the Supreme Court in an unreported order,⁵¹ the third and fourth judgements which were pronounced more recently in 2020 and 2022 have sustained and continue to be valid law. Now, we consider the applicability of the aforementioned rationale in arguing for extending personhood to AI. The first rationale for expanding personhood which we can cull out from the cases reviewed above is that juristic personhood originates out of religious belief/ faith of the society and upon performance of religious ceremonies. Now, authors have talked about how Artificial Intelligence could significantly impact the way people perceive and study religion,⁵² and have also gone to the extent of arguing that it would be reasonable to expect religion to accept, integrate and co-exist with AI in the future.⁵³ In the event of such a situation actualizing, if AI attains the level of sanctity that is attributed to stone and wooden figures which are consecrated as images of gods, then this non-legal but religious line of reasoning can be relied on to accord personhood to AI. This would also bring forth consequences specifically for modification of property relations *vis-a-vis* AI on the lines of what was seen in the *Ram Jankijee Deities v State of Bihar* case mentioned earlier. However, the existing state-of-the-art is still miles away from such a situation.

Similarly, a second line of reasoning used in these cases for justifying the expansion of personhood to cover non-natural entities, is that such expansion would be necessary to meet the needs of human development. This argument is founded on the conception that with societal development, social and commercial relationships take on newer forms and are even established through the means of non-human entities, necessitating the recognition of their personhood to facilitate the legal enforcement of such relationships.⁵⁴ From this line of reasoning follows the argument that it is important to recognize the personhood of rivers because the lives and livelihood of fisher-folk, boatsman etc. are invariably tied to the river and their socio-economic relationships are manifested through it.

⁵¹ *State of Uttarakhand v Mohd. Salim* (2017) SCC OnLine SC 903.

⁵² Randall Reed, 'A.I. in Religion, A.I. for Religion, A.I. and Religion: Towards a Theory of Religious Studies and Artificial Intelligence' (2021) 12 *Religions* 401 <<https://doi.org/10.3390/rel12060401>> accessed 9 April 2026.

⁵³ Toomas Meema, 'Religion and Artificial Intelligence' (Tartu Ülikool 2018) <<https://dspace.ut.ee/items/a3c2f92e-fd8d-472b-95bd-5a6323cfabd3>> accessed 9 April 2026.

⁵⁴ Joffrey Baeyaert, 'Beyond Personhood: The Evolution of Legal Personhood and Its Implications for AI Recognition' (2025) *Technology and Regulation* 355 <<https://techreg.org/article/download/22555/25839/63145>> accessed 9 April 2026.

This second argument can be abstracted to apply to AI in two ways. Firstly, we are at a stage of scientific development where, because of methods like deep learning⁵⁵ and usage of black boxes, the output that an AI produces or a decision it makes cannot be directly attributed to any specific natural person or traced through a human developed code.⁵⁶ As a result, it is difficult to place the responsibility on either the user or the creator of the AI. And because of such scientific advancements, it is necessary to recognize AI itself as an author by granting it juristic personhood *for the sake of ease of pursuing commercial and legal relationships and resolving questions of liability*.⁵⁷ Secondly, borrowing from David Gunkel's arguments, we can say that AI developers and AI operators *express their socio-economic relationships through the means of AI* and thus it is necessary to recognize AI as a juristic person so that we can fit it better into our social world. To instantiate this, we can consider Gunkel's example of recognition of how some states in the US have recognized the pedestrian rights of delivery robot- seen as motivated by the necessity to serve socio-scientific developmental needs.⁵⁸

Lastly, a third line of justification that is seen as being used in these cases is based on the idea that juristic personality can be extended to entities which act like natural persons, i.e., to scientifically or biologically living entities. This third argument is especially useful when dealing with Artificial General Intelligence and Strong AI which are definitionally understood as AI that can match the level of intellectual capacity and self-awareness that humans possess.⁵⁹ Researchers writing as far back as 2013 have noted the promising prospects offered by studies in Artificial Life or 'Alife' in artificially crafting and simulating biological life.⁶⁰ Taking note of these strong strides being made towards creation of AI that closely resembles human capacity, it is definitely plausible that arguments may be made based on the bio-equivalence of AI to seek recognition of its personhood.

This exercise of abstracting the arguments thus provides us with a broad idea and a blueprint of the trajectory that the legal validation of AI personhood could take in the future. As can be seen, these case laws and the rationale used therein to expand the idea of personhood from

⁵⁵ Vikas Hassija and others, 'Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence' (2023) 16 *Cognitive Computation* 45 <<https://doi.org/10.1007/s12559-023-10179-8>> accessed 9 April 2026.

⁵⁶ Brian Judge, Mark Nitzberg and Stuart Russell, 'When code isn't Law: Rethinking Regulation for Artificial Intelligence', *Policy and Society* (2025) Volume 44, Issue 1, 85–97, <<https://doi.org/10.1093/polsoc/puae020>> accessed 9 April 2026.

⁵⁷ David J Gunkel, 'The Relational Turn: Thinking Robots Otherwise' (2022) *SSRN Electronic Journal*.

⁵⁸ Gunkel D, 'Person, thing, robot: A moral and legal ontology for the 21st century and beyond' (2023) *MIT Press*.

⁵⁹ Stuart J Russell, *Human Compatible: Artificial Intelligence and the Problem of Control* (Penguin Books 2020).

⁶⁰ Ben Goertzel, 'Artificial General Intelligence: Concept, State of the Art, and Future Prospects' (2014) *Journal of Artificial General Intelligence* 1 <https://ui.adsabs.harvard.edu/link_gateway/2014JAGI....5....1G/doi:10.2478/jagi-2014-0001> accessed 9 April 2026.

strictly human/ corporate entities to cover even non-sentient environmental entities, have been formulated in a manner that gives ample space for grafting the same arguments over to the context of AI personhood as well. What remains to be seen is how the development and future evolution of AI take place, for it to fit into this trajectory.

VI. CONCLUSION AND WAY FORWARD

In Episode 9 titled ‘The Measure of a Man’⁶¹ of the second season of the popular American TV show Star Trek, an artificially intelligent android named Data is put to trial to decide on whether it should be deemed a legal person. The hearing proceeds with Commander Maddox, who seeks to have Data declared to be a mere property and not a person in itself, arguing that since Data is not a sentient being, he is not entitled to any rights. On the other hand, Captain Piccard, arguing in favour of recognizing Data’s personhood, counters Maddox’s contention by asking him *what is required for sentience*. “Intelligence, self-awareness, consciousness.” Maddox replies. And the rest of the hearing unfolds with Captain Piccard successfully arguing how Data can demonstrate both intelligence and self-awareness and thus meets two of the three criteria required to qualify as a sentient being. With the third criteria left not proved, the court rules in favour of Captain Piccard and upholds the recognition of Data’s legal personhood.

In what has turned out to be an extremely foresightful prediction of the AI-personhood puzzle we are faced with today; the episode demonstrated how, at least the literary imagination on legal personhood of artificial intelligence had long evolved beyond the limits of biological status. To that end, this paper has been an exercise in trying to understand the plausibility of fact imitating fiction, in the context of recognition of AI personhood under Indian jurisprudence. While in recent times, there has been substantial scholarship trying to portend the legal trajectory in this regard, the above analysis sought to push the boundaries of *legal imagination* in framing arguments for extending legal personhood to AI by referring to an under-explored connection between technology and environmental law. Although much less discussed in both AI and environmental research, both these domains of law are intertwined to the extent that they both seek to regulate and create frameworks for governance of technological and industrial developments and thus these areas of research have much to inform and learn from each other. To that extent, this paper hopes to forge new conversations on how AI regulation can integrate theories of environmental law. The research has highlighted the

⁶¹ ‘The Measure of a Man’, Star Trek: The Next Generation (*Netflix*, 2025), Season 2, Episode 9.

how the recognition of AI personhood may necessitate a reformulation of existing jurisprudential boundaries and simultaneously how, such designation of personhood can be reconciled with existing theories continuing debates on personhood of other non-human entities like rivers, lakes and the environment. This analysis can further lay the foundations for research in how, such an abstraction of personhood theory to extend it to AI, can be reconciled with the tenets of the Constitution to ensure legislations recognizing AI personhood do not fall foul of its basic structure.

DIGITAL SOVEREIGNTY AND MACROECONOMIC RESILIENCE: ANALYSING INDIA'S REGULATORY FRAMEWORK FOR DIGITAL CURRENCIES

—Bhagyashree Tiwari*

ABSTRACT

The rapid proliferation of digital currencies presents a structural challenge to India's framework of monetary sovereignty, capital flow management, and financial stability. This paper analyses vulnerabilities in India's legal and regulatory architecture as they pertain to monetary policy, exchange rate management, and banking intermediation. It argues that India has adopted a calibrated model of regulatory deterrence rather than pursuing either a blanket prohibition or full regulatory accommodation of private digital assets. Through an examination of the Reserve Bank of India Act, 1934, the Income Tax Act, 1961, the Foreign Exchange Management Act, 1999, and the application of anti-money laundering obligations, the paper demonstrates how India simultaneously discourages speculative crypto asset activity while advancing a sovereign alternative through the Digital Rupee. The analysis further shows that this fragmented framework generates regulatory ambiguity, particularly in relation to cross-border transactions and capital account classification. It contends that unless India transitions toward a coherent statutory regime that clearly classifies digital assets and aligns regulatory jurisdiction, the effectiveness of its macroeconomic policy tools will remain constrained.

Keywords: Digital Currency, Monetary Sovereignty, Regulatory Deterrence, Foreign Exchange Management Act, Central Bank Digital Currency, Financial Stability.

* Bhagyashree Tiwari is a student at National Law University, Jodhpur (NLUJ).

I. INTRODUCTION TO INDIA'S DIGITAL CURRENCY IMPERATIVE

A. *The Context: The Global Digital Money Revolution and the Problems Posed to State Authority*

The financial ecosystem across the globe is undergoing a significant change driven by digital tokens. This shift has come along with unique and novel challenges to the traditional view of monetary sovereignty, which provided for the States exclusive control over its currency and monetary policy. Central banks have traditionally exercised exclusive control over the issuance, flow, and valuation of currency, regulating money supply, interest rates, and credit within the economy. However, this monopoly is now being challenged by the emergence of privately issued digital currencies (“DC”), which operate in parallel markets and provide alternative avenues of access to monetary value outside the formal banking system.

This brings us to the conflict faced by the State authorities between encouraging financial innovation, like faster payments, enhanced inclusion and better efficiency, and preserving the stability of the national monetary system established by integrity and central control. The Reserve Bank of India (“RBI”) has explicitly cautioned about the necessity to reserve currency issuance to the State and has actively promoted a sovereign Central Bank Digital Currency (“CBDC”) while maintaining scepticism regarding uncontrolled private digital assets.¹

B. *The Digital Currency Triad of Central Bank Digital Currency, Unbacked Cryptocurrency, and Stablecoins*

The present paper focuses on three forms of DC: CBDC, Unbacked Crypto, and Stablecoins. Before delving into the legal and economic understanding, it is necessary to talk about the technical meaning of these currencies. First, there is CBDC, which is a state-backed solution to this problem. Digital Rupee (₹), for example, is the liability of the central bank issued in a digital form and it is exchangeable at par with the existing currency. It enjoys the status of a legal tender and zero credit-risk status as that enjoyed by money in physical form.² Conceptually, currency, whether physical or digital, is fundamentally a legal construct. It is a form of legal tender issued under sovereign authority and represents a liability of the State (or

¹ Siddharth Upasani, RBI Governor Malhotra Urges Other Central Banks to Promote CBDCs Over Stablecoins *The Indian Express*, (16 October 2025) <<https://indianexpress.com/article/business/rbi-governor-malhotra-urges-central-banks-promote-cbdc-stablecoins-10309697/#:~:text=Reserve%20Bank%20of%20India%20%28RBI%29%20Governor%20Sanjay%20Malhotra,%28CBDCs%29%20instead%20of%20stablecoins%20to%20facilitate%20international%20payments>> accessed 1 November 2025.

² Reserve Bank of India, Concept Note on Central Bank Digital Currency (October 2022) <<https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CONCEPTNOTEACB531172E0B4DFC9A6E506C2C24FFB6.PDF?>> accessed 3 November 2025.

Central Bank). Its acceptance is not based on intrinsic value but on legal recognition and public trust in the sovereign. Second, there are Unbacked Cryptocurrencies, for example, Bitcoin, which are decentralised, highly volatile, non-government-issued, and non-government-backed. They are legally termed as Virtual Digital Assets (“VDA”) under Section 2(47A) of the Income Tax Act, 1961 (“IT Act”).³ Importantly, this definition explicitly excludes VDA from being treated as Indian or foreign currency and firmly isolates it from the monetary base.

Third, there are Stablecoins, which are “*a class of crypto-assets designed to maintain a stable value by pegging themselves to a reference asset, such as a fiat currency, commodity, or basket of assets. They are typically issued by private entities and achieve price stability either through reserve backing or algorithmic mechanisms. Functionally, they enable relatively stable, transferable value on blockchain-based infrastructure, often facilitating payments and trading within the crypto ecosystem.*”⁴ The Bank for International Studies (“BIS”) has warned that foreign stablecoins risk replacing domestic currencies and compromising the policy sovereignty of central banks.⁵

C. Indias Policy of Balancing Innovation, Inclusion and Stability

The Indian policy approach is structured around dual objectives. On one hand, there is always a push for innovation and financial inclusion, which is evident by the accelerated development of the Digital Rupee. With its recent offline functionality pilots, the RBI aims to maximise its reach in rural areas as well. The digital alternative is designed to work in conjunction with payment infrastructures like UPI.⁶

On the other hand, the overriding objective is the preservation of stability and monetary sovereignty. The RBI has clearly stated that the scepticism towards private cryptos is based on them having no underlying cash flow, no issuer and thereby having no value.⁷ Further, the RBI retains the philosophy regarding capital account convertibility, viewing it as a gradual process

³ The Income-tax Act, 1961 (43 of 1961) s 2(47A).

⁴ INTERNATIONAL MONETARY FUND, Monetary and Capital Markets Department – Understanding Stablecoins, DEPARTMENTAL PAPER (2025).

⁵ Bank for International Settlements, Central Bank Digital Currencies (CBDC) in Emerging Market Economies (EMEs) – India BIS Papers No. 123 (April 2022) <https://www.bis.org/publ/bppdf/bispap123_j.pdf#:~:text=Finally%2C%20securing%20monetary%20sovereignty%20is,risk%20of%20%E2%80%9Ccryptocurrencies%E2%80%9D%20and%20foreign> accessed 3 November 2025.

⁶ The Economic Times, Discussions on with RBI over Digital Currency: Nirmala Sitharaman (14 February 2022) <<https://economictimes.indiatimes.com/news/economy/policy/discussions-on-with-rbi-over-digital-currency-nirmala-sitharaman/articleshow/89565439.cms>> accessed 1 November 2025.

⁷ Srijashree Sardar et.al., Decentralised Finance: Implications for Financial System Reserve Bank of India Bulletin (May 2024) <https://www.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=22588> accessed 2 November 2025.

and not an event as such. So, the approach is that of strict control over outward capital flows threatened by borderless crypto channels. DC are beginning to fundamentally change macroeconomic policy by challenging the traditional tools of monetary and financial regulation.⁸ Their large-scale adoption, especially of foreign Stablecoins, risks distortion of key monetary aggregates and reduces the RBI's capacity to manage liquidity. Moreover, it would allow for cross-border crypto transactions, facilitating stealth capital flight. It can destabilise the exchange rate and weaken the enforcement of legislation controlling capital flow management.⁹ At the same time, DCs may alter the structure of financial intermediation by affecting bank deposits, credit creation, and systemic stability, especially during periods of stress. These issues are explored in detail in the sections that follow, which examine the implications of DCs for monetary sovereignty, financial stability, and regulatory design.

II. THE LEGAL FRAMEWORK OF INDIA'S DIGITAL MONETARY SYSTEM

A. The Reserve Bank of India Act, 1934 and Legalisation of the Digital Rupee (₹) as Sovereign Liability

The foundation of India's monetary control rests on the exclusive authority granted to the RBI under the RBI Act, 1934. Section 22 gives it the exclusive right to issue banknotes in India.¹⁰ Till recently, this definition was limited to physical paper currency.¹¹ However, in 2022, the Finance Act amended the RBI Act and inserted Section 26A,¹² explicitly stating that banknote includes its digital form, thereby legitimising CBDC and empowering the RBI to issue it.¹³ This change established Digital Rupee (₹) as a legal tender with the guarantee of the Central Government. It was given the same sovereign status as physical cash. This reinstated the central banks monopoly and preserved the states ultimate control over the currency issue mechanism.

⁸ Julien Brault & Patrick McKeon, Capital Controls and Cryptocurrency Trading (2023) 75 J. Intl Money & Fin. 102198.

⁹ Dmitry Sergeyev & Guido Friebel, Cryptocurrency Adoption and Capital Controls CESIFO WORKING PAPER No. 9876 (2023).

¹⁰ The Reserve Bank of India Act, 1934 (2 of 1934) s 22.

¹¹ Lakshmikumaran Sridharan Attorneys, Trading in Virtual Currencies: An Analysis Under Foreign Exchange Laws of India (3 April 2018) <<https://www.lakshmisri.com/insights/articles/trading-in-virtual-currencies-an-analysis-under-foreign-exchange-laws-of-india/#:~:text=or%20any%20other%20authority%20empowered,bitcoins%20are%20not%20%E2%80%98bank%20notes%E2%80%99%99>> accessed 30 October 2025.

¹² The Reserve Bank of India Act, 1934 (2 of 1934) s 26A.

¹³ The Finance Act, 2022 (6 of 2022) s 139.

However, it explicitly excluded private cryptocurrencies, not issued or backed by the RBI, from attaining the status of a sovereign currency.¹⁴

B. Virtual Digital Assets under the Income Tax Act, 1961 and their Classification as Property, not Currency

There is no dedicated regime for private crypto. The IT Act, 1961, has provided the first statutory recognition of these assets, although strictly for fiscal purposes.¹⁵ The 2022 Budget introduced Section 2(47A), defining VDA broadly to include “any token or instrument generated through cryptography, notably not being Indian currency or foreign currency”.¹⁶ This definition provided a mechanism for regulatory containment through fiscal deterrence.

The 30% punitive tax on Deep Value Asset (“DVA”) profits, with a 1% Tax Deducted at Source (“TDS”), imposed robust fiscal sanctions for trading on speculation. This has been actively enforced and has generated substantial amounts of revenue; the government reported that it collected ₹437 crore in taxes from DVA income in FY 2022-23.¹⁷ This model effectively recognises the existence and tradability of the asset (for tax collection) while simultaneously denying it legitimacy as a currency. Judicial interpretation supports this view, with the Madras High Court in 2023 holding that virtual coins are goods or property under the Sale of Goods Act, indicating they are tradable, but not legal tender.¹⁸

C. Controlling Cross-Border Flows and the Foreign Exchange Management Act, 1999

The legal status of VDA under the Foreign Exchange Management Act, 1999 (“FEMA”), which governs capital and currency flows, remains highly ambiguous with significant compliance challenges.¹⁹ Cryptocurrencies fall in the regulatory grey zone under FEMA. Legal professionals are increasingly treating VDA purchases on foreign platforms as capital account transactions, those that change a country’s assets or liabilities with the rest of the world, for FEMA and, therefore, require RBI approval, thereby resembling the acquisition of intangible

¹⁴ The Economic Times, India to Launch Digital Currency, says Piyush Goyal; Discourages Cryptocurrency “Not Backed by Assets” (7 October 2025) <<https://economictimes.indiatimes.com/markets/cryptocurrency/india-to-launch-digital-currency-says-piyush-goyal-discourages-cryptocurrency-not-backed-by-assets/articleshow/124351395.cms>> accessed 30 October 2025.

¹⁵ The Income-tax Act, 1961 (43 of 1961).

¹⁶ IT Act (n 3).

¹⁷ The Economic Times, Crypto tax nets ₹437 crore in FY23; govt collects ₹3,000 crore in TDS so far (23 July 2023) <<https://economictimes.indiatimes.com/tech/technology/crypto-tax-nets-rs-437-crore-in-fy23-govt-collects-rs-3000-crore-in-tds-so-far/articleshow/102012807.cms>> accessed 2 November 2025.

¹⁸ *Rhutikumari v Zanmai Labs Pvt. Ltd. & Ors.* (Mad.) O.A. No. 194 of 2025, 2025 MHC 2437.

¹⁹ The Foreign Exchange Management Act, 1999 (42 of 1999).

assets outside of the Indian economy.²⁰ If this interpretation is correct, the legality of acquiring such virtual digital assets from the platforms service provider using other channels in India's regulatory framework, such as the Liberalised Remittance Scheme, is unclear and in violation of Indian laws. The legal ambiguity acts as a sort of soft capital control, allowing entities to treat outflows of cryptocurrency as prohibited capital transactions. Additionally, if the Prevention of Money Laundering Act, 2002 ("PMLA") is applied to digital asset service providers Anti-Money Laundering ("AML") and Know Your Customer ("KYC") regulations, the PMLA may act as a key regulatory checkpoint for monitoring and limiting dark financial flows.²¹

D. Legal Precedents and Regulatory Gaps

The case of *Internet and Mobile Association of India v. RBI* in 2020 was a notable point in the evolution of the regulatory framework.²² The Supreme Court of India on March 4, 2020, took down the RBI's 2018 circular that prohibited banks "from providing services to crypto exchanges, ruling that the blanket ban was disproportionate."²³ In the order, the court acknowledged the RBI's authority to regulate digital currencies as payment instruments; however, it suggested that less restrictive regulatory methods be attempted.²⁴

Despite this judicial order, as of the end of 2025, there is no extensive, dedicated statute that governs licensing or prudential regulation of private crypto exchanges. The existing regulatory framework remains a patchwork model that marries judicially protected trade, tax levied on gains, and active reliance on AML/PMLA. There is little likelihood of this gap being addressed because, while draft legislation has been floated for consideration, the government instead has favoured focus on the sovereign digital rupee and partial oversight on private crypto due to concerns of systemic risk.

²⁰ Maniraj Anantham, How FEMA Impacts Crypto & Virtual Digital Assets in India: A Complete Guide Tax Robo (7 September 2025) <<https://blog.taxrobo.in/fema-impact-on-crypto/>> accessed 3 November 2025.

²¹ The Prevention of Money Laundering Act, 2002 (15 of 2002).

²² *Internet and Mobile Association of India v RBI* AIR 2021 SC 2720.

²³ *Id.*; Rohan Bagai et.al., Virtual Currency Regulation Review 2025 AZB & Partners (12 June 2025) <<https://www.azbpartners.com/bank/virtual-currency-regulation-review-2025/#:~:text=The%20RBI%20Directive%20was%20later,6>> accessed 2 November 2025.

²⁴ Nakul Dewan & Rohan Andrew Naik, Lets Trade Crypto: Indian Supreme Court Quashes Prohibition Oxford Business Law Blog (19 March 2020) <<https://blogs.law.ox.ac.uk/business-law-blog/blog/2020/03/lets-trade-crypto-indian-supreme-court-quashes-prohibition#:~:text=The%20Court%20accepted%20the%20submission,more%20proportionate%20response%20than%20prohibition>> accessed 1 November 2025.

III. THE MACROECONOMIC RISKS ON THE WAY

A. Capital Flight and Exchange Rate Management

The emergence of DC presents an immediate macroeconomic challenge to India by undermining the capital control framework, which permits liberalised inflows but manages outflows via tighter controls of the regulated routes under FEMA.²⁵ Crypto marketing platforms circumvent capital controls in the economy by allowing near-instant and largely pseudonymous cross-border transfers that exist outside authorised paths. Studies cited in Yale Journal on Regulation have shown that trading volumes of crypto assets are higher in capital-controlled domestic economies, indicative of their use to evade capital controls.²⁶ For India, capital account liberalisation is intended to be gradual and through controlled supervision of the capital flows in/out of the economy. The advent of unregulated digital routes for transactions dilutes the effectiveness of capital account liberalisation policy as to of balance of payments and financial regulation.

Stablecoins, especially those that are pegged to the foreign bank, the US dollar, increase the potential for residents to engage in cryptoization, whereby residents become increasingly comfortable transacting or saving in digital currencies for future use rather than the local currency.²⁷ An exchange of Rupees for stablecoins diminishes local liquidity for domestic transactions as corresponding reserve assets (US Treasuries, typically) are maintained outside the economy, creating capital outflows that, while not recorded, are still capital outflows. At scale, these dynamic yields foreign exchange pressures to depreciate the Indian Rupee, increase volatility, and inhibit the ability of the RBI to maintain exchange rates and monetary policy.

B. Monetary Policy Effectiveness and Inflation

The efficacy of monetary policy rests on the ability of the central bank to track and control the money supply. However, if DC becomes widely adopted, it could lessen control over the money supply by distorting traditional monetary aggregates such as M1 (Narrow Money) and M3 (Broad Money).²⁸ Here, M1 is the most liquid money, including cash and demand deposits, used for daily transactions. M2 includes M1 plus savings deposits and short-term deposits. M3

²⁵ Reserve Bank of India, Report of the Committee to Review the Facilities for Individuals under the Foreign Exchange Management Act, 1999 (July 2013).

²⁶ G. Eichengreen, Will Central Bank Digital Currencies Doom Dollar Dominance? 35 Yale J. Reg. F. 202 (2023).

²⁷ Tobias Adrian, The Changing Landscape of Crypto Assets- Considerations for Regulatory and Supervisory Authorities IMF-FSB-OCC Crypto Conference (23 February 2024)

<<https://www.imf.org/en/News/Articles/2024/02/23/sp022324-changing-landscape-crypto-assets-considerations-regulatory-and-supervisory-authorities>> accessed 4 November 2025.

²⁸ BIS CBDC (n 5).

is the broadest measure, covering M2 along with large deposits and other less liquid financial assets. If consumers increasingly hold or transact in foreign-pegged stablecoins, the effective liquidity circulating in the economy may be higher than official measures suggest, creating policy blind spots. This diminishes the RBI's capacity to manage liquidity through repo rate changes, or open market operations - thus weakening both monetary transmission and inflation targeting. As substitution into non-rupee tokens increases, the RBI's ability to anchor prices in its 4 per cent inflation target band becomes even more tenuous.²⁹

Further, the emergence of stablecoins exposes the domestic economy to external monetary shocks and imported inflation. When residents shift some of their savings into US dollar-backed digital coins - usually as a reactionary response to perceived domestic inflation or ongoing policy uncertainty - it signals less confidence in the rupee and effectively imports US monetary conditions directly into the Indian economy.³⁰ This phenomenon undermines the overall autonomy of the RBI and amplifies the challenges associated with stabilising prices. Notably, the Digital Rupee (e₹) exists as a strategic and policy countervailing force, that has the capacity to restore visibility and control over the digital money supply. It is needed to ensure that its deployment respects privacy standards under the Digital Personal Data Protection Act, 2023 (“DPDPA”).³¹

C. Financial Stability and Banking Intermediation

Under normal circumstances, the efficiency and convenience of CBDCs and stablecoins will allow deposits to gradually migrate from banks (to their wholesale funding sources) and diminish overall credit growth rates. However, during a time of distress in the markets, this process may manifest suddenly as the extremely riskless and highly transferable CBDC quickly permits instant, cash-funded digital bank withdrawals and intensifies the risk of systemic bank runs. Fast disintermediation will present emerging economies like India with an extraordinary problem, particularly in a system where banking stability drives the expansion of credit and resilience of the macroeconomy.³²

To alleviate this risk, RBI has intentionally designed the Digital Rupee (e₹) such that financial stability takes precedence over adoption. The e₹ is non-interest-bearing, so it is not a close substitute for savings deposits, and there are Prudential holding caps (e.g., ₹1,00,000 maximum wallet size) that limit e₹ transfer from banks into other financial institutions during distress.

²⁹ RBI Concept Note (n 2).

³⁰ *Decentralised Finance* (n 7) 243–46.

³¹ The Digital Personal Data Protection Act, 2023 (22 of 2023).

³² Tobias Adrian (n 27).

The careful development of the e₹ creates balance between innovation and prudence, even if it potentially decelerates the rate of adoption.³³ Additionally, the RBI curates a strict firewall between the regulated banking system and its volatile private cryptocurrencies, as it imposes AML/KYC requirements under the PMLA to limit contagion potential.

The e₹ is also being strategically used to promote financial inclusion with pilot programs extending offline use to areas with low connectivity. However, a transaction limit of ₹200 per transaction and ₹500 cumulatively signals the RBI's continuing priority to mitigate operational risk and prevent fraud, ensuring that innovation does not jeopardise the integrity of the system. Despite these significant macroeconomic risks, the existing legal and regulatory framework remains fragmented and largely reactive, struggling to adequately capture the scale, speed, and cross-border nature of digital currencies. Traditional tools under FEMA, monetary policy, and banking regulation were not designed for decentralised and privately issued digital assets, leading to gaps in oversight and enforcement. It is within this backdrop of regulatory insufficiency that India's current strategy, combining deterrence with calibrated digital innovation, needs discussion.

IV. INDIA'S REGULATORY STRATEGY: DETERRENCE AND DIGITAL DEPLOYMENT

A. The Role of Taxation and AML/PMLA Compliance

India's regulatory stance on private VDAs is driven by deterrence through fiscal and regulatory pressure as opposed to a total ban. The 30% tax on VDA gains and the 1% TDS on transactions, implemented in 2022, serve as robust disincentives to speculative trading while also providing a new avenue for fiscal visibility, monetising ₹437 crore in 2022 - 23.³⁴ In addition, exchanges are required to register with the Financial Intelligence Unit and comply with KYC and transaction monitoring obligations under the PMLA, thereby introducing regulatory friction that reduces anonymity and helps deter illicit financial flows.³⁵ Together, these strategies do

³³ Nikhunj Ohri & Sarita Chaganti Singh, Exclusive: India Resists Full Crypto Framework, Fears Systemic Risks, Document Shows Reuters (10 September 2025) <<https://www.reuters.com/world/india/india-resists-full-crypto-framework-fears-systemic-risks-document-shows-2025-09-10/#:~:text=Indians%20have%20investments%20worth%20%244,financial%20stability%2C%20the%20document%20said>> accessed 30 October 2025.

³⁴ The Hindu, 30% tax, 1% TDS on crypto transactions come into effect (1 April 2022) <<https://www.thehindu.com/business/Economy/30-tax-1-tds-on-crypto-transactions-comes-into-effect/article65283602.ece>> accessed 1 November 2025.

³⁵ Press Release, Fin. Intelligence Unit–India, FIU-IND Issues Compliance Show Cause Notice to Binance (28 December 2023) <<https://fiuindia.gov.in>> accessed 2 November 2025.

create a controlled tolerance framework where oversight is mitigated, but the use of VDAs is not sanctioned as a form of currency.

B. The Digital Rupee (e₹)

The RBI has rolled out its CBDC in phases, with a two-pronged strategy - wholesale (e₹-W) targeting institutional efficiencies and retail (e₹-R) targeting gradual consumer take-up.³⁶ The wholesale CBDC is clearly emerging with a positive start, as transactions expanded quickly from ₹57 million (FY 2022-23) to ₹2.34 billion (FY 2023-24) as a way to reduce cost in interbank transactions.³⁷ Retail take-up of the CBDC has been deliberately slow, limited by the controls of a non-interest-bearing wallet with a product limit of ₹1,00,000, as a means to protect bank intermediation.³⁸ The introduction of a sovereign digital infrastructure on the wholesale side has allowed the RBI to contain speculative VDA investment through taxation and AML. These measures have allowed India's central bank to promote Digital Dualism, a regulatory approach where innovation in digital finance is encouraged alongside parallel safeguards to preserve financial stability and control, and systematic innovation through digitalisation, while maintaining financial stability.³⁹

C. The Potential for a Regulated INR-Backed Stablecoin

As the RBI appears to remain hesitant toward foreign stablecoins, there are ongoing discussions about the possibility of a fully regulated, INR-backed stablecoin. This stable coin would be regulated on the value of an underlying government security or fiat reserves under the statutory responsibility of the RBI, a regulatory role.⁴⁰ This type of token would create a hybrid of digital efficiency and monetary sovereignty by empowering experimental currency cross-border settlement mechanisms and protecting existing monetary currency mechanics. Ultimately, this would more actively entrench the indigenous role of the rupee internationally. In effect, this type of innovation would not only compete with foreign stablecoins, but it could also prevent

³⁶ Synergia Legal, Visualising the Digital Rupee: Legal Foundation for India's CBDC, <<https://synergialegal.com/visualizing-the-digital-rupee-legal-foundation-for-indias-cbdc/>> accessed 7 November 2025.

³⁷ Times of India, RBI to explore cross-border CBDC pilots as e-rupee circulation surges to ₹1,016 crore (29 May, 2025) <<https://timesofindia.indiatimes.com/business/india-business/e-rupee-circulation-rises-to-rs-1016-crore-rbi-to-explore-cross-border-cbdc-pilots/articleshow/121493447.cms>> accessed 5 November 2025. .

³⁸ Abhijeet Kumar, RBI DY Guv Reaffirms Crypto Scepticism, Says CBDC Will Grow Step by Step (30 October 2025) <https://www.business-standard.com/specials/bs-events/rbi-crypto-stance-cbdc-calibrated-growth-dy-guv-rbi-sankar-125103000943_1.html> accessed 5 November 2025.

³⁹ Jasdeep Kaur, Central Bank Digital Currency – The digital rupee in India, EngageEcon. Political Weekly, (5 September 2023).

⁴⁰ Fin. Stability Bd., High-Level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements (17 July 2023) <<https://www.fsb.org/wp-content/uploads/P170723-3.pdf>> accessed 6 November 2025.

the potential future dollarisation of the Indian economy.⁴¹ There are similar discussions and models around the world, such as proposals from China for stablecoins backed by their currency to increase the usage of their currency in the international economy.⁴²

V. COMPARATIVE POLICY ANALYSIS AND GLOBAL BENCHMARKING

A. *The European Model: MiCA*

The European Union's Markets in Crypto-Assets Regulation ("MiCA") adopted in 2023, offers a harmonised framework which prioritises regulation over complete prohibition.⁴³ It mandates uniform licensing, capital adequacy, and consumer protection and also addresses the monetary risks posed by stablecoins. MiCAs reserve requirements for Asset-Referenced and E-Money Tokens ensure that the issuers maintain fully backed, segregated and liquid reserves. For India this provides a replicable model mandating that any rupee-pegged stablecoin be backed by reserves held domestically to be under RBI supervision.⁴⁴ This reconciles innovation with monetary sovereignty.

B. *The Chinese Model: Centralised Control via E-CNY and Complete Crypto Ban*

Chinas model entails absolute regulatory centralisation. China banned private crypto-trading and mining in 2021, and ever since, it has consolidated its monetary control through the e-CNY, a fully sovereign CBDC designed for domestic retail use and managed anonymity.⁴⁵ This e-CNY not only secures their internal financial stability but also serves their broader strategy of Renminbi internationalisation through potential Yuan-backed stablecoins for cross-border use.⁴⁶ China, thus, enforces digital autarky. Chinas model is non-transferable to India because Indias constitutional framework, commitment to economic freedoms, and market driven financial system limit the feasibility of strict state control and blanket prohibitions on private

⁴¹ *Decentralised Finance* (n 7).

⁴² Martin Chorzempa, Chinas "Digital Currency Revolution": Implications for the Global Financial System Peterson Inst. for Intl Econ. Policy Brief 21-22 (August 2021).

⁴³ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets, OJ L 150/40.

⁴⁴ IMF & Fin. Stability Bd., IMF-FSB Synthesis Paper: Policies for Crypto-Assets (7 September 2023), <<https://www.fsb.org/wp-content/uploads/R070923-1.pdf>> accessed 7 November 2025.

⁴⁵ Peoples Bank of China et al., Notice on Further Preventing and Disposing of the Risk of Speculation in Virtual Currency Trading (P.R.C.) (24 September 2021).

⁴⁶ Peoples Bank of China, Progress of Research & Development of e-CNY (White Paper) (July 2021), <<https://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>> accessed 6 November 2025.

digital assets. Indias hybrid approach of combining fiscal deterrence with CBDC deployment represents a pragmatic middle path within this global policy continuum.

C. The Data Gaps Initiative and Indias G20 Presidency

At the global level, India leveraged its G20 Presidency of 2023 to build consensus on global crypto regulation, culminating in the IMF-FSB Synthesis Report of 2023 that advocates for reserve-backed stablecoins and cross-border regulatory coordination.⁴⁷ Complementing this, the Data Gaps Initiative (DGI-3) led by the IMF,⁴⁸ FSB and BIS highlights the inadequacy of existing macroeconomic statistics in capturing actual crypto-related capital movements and currency substitution.⁴⁹ This validates the RBIs caution that unrecorded digital flows pose hidden systemic risks. Thus, Indias advocacy for a shared global standard and coordinated supervision aligns with its domestic objective of safeguarding monetary and macro-financial stability in an increasingly digitised economy.⁵⁰

VI. RECOMMENDATIONS AND CONCLUSION

The rise of digital currency has prompted India to find a precarious balance between financial innovation and macroeconomic stability. Private VDAs and foreign-pegged stablecoins emerge as a challenge to Indias managed monetary framework by muddying monetary policy transmission, facilitating regulatory capital outflows, and putting exchange rate stability at risk. The current policy set-up, based on taxing gains from VDAs, placing PMLA obligations on crypto intermediaries, and the pilot launch of the Digital Rupee (e₹), is a pragmatic response but still deficient. These reforms are indicative of a transitional regulatory deterrence strategy, which seeks to mitigate risks without legitimising private digital currencies. However, systemic vulnerabilities continue to exist because of a lack of a clear and targeted legal framework as it pertains to cross-border crypto transactions, especially under FEMA, and the uncertainty of classifying these transactions as capital account transactions remains.⁵¹ This serves as a form of indirect control, but is insufficient compared to legislative guidance under a clear and explicit legal framework. Ultimately, private stablecoins are both a policy problem and an

⁴⁷ IMF-FSB (n 44).

⁴⁸ Intl Monetary Fund, People, Planet, Economy: Third Phase of the G20 Data Gaps Initiative (DGI-3) — First Progress Report (October 2023) <<https://www.imf.org/-/media/Files/News/Seminars/DGI/Documents/third-phase-of-the-data-gaps-initiative-first-progress-report.ashx>> accessed 7 November 2025.

⁴⁹ *Stablecoin Recommendations* (n 40).

⁵⁰ *BIS CBDC* (n 5).

⁵¹ *Maniraj Anantham* (n 20).

accelerator of innovation for the RBI as it determinedly works to develop sovereign digital alternatives.

To ensure macro-financial stability, India should pursue an integrated legislative and regulatory regime. A Crypto-Asset Regulation Act should be developed, which would define classes of digital assets, such as utility tokens, security tokens, and stablecoins, and delineate regulatory jurisdiction between the RBI and SEBI. This Act should explicitly state that private cryptocurrencies will not be legal tender but will establish a regulated and transparent operating environment for compliant entities. Issuance and use of stablecoins by Indian residents, for example, should be contingent upon obtaining explicit RBI approval, and reserve assets should be required to be maintained in India. In addition, the FEMA should be amended to expressly include digital assets within its regulatory scope. Specifically, Section 2(e) (definition of capital account transaction) and Section 2(u) (definition of security) should be expanded to cover virtual digital assets, and corresponding rules should be updated. This would clarify that cross-border acquisition or transfer of cryptocurrencies constitutes a capital account transaction, requiring RBI approval or routing through authorised persons, along with mandatory reporting and disclosure requirements.⁵² Implementation of these legislative and regulatory reforms will close the enforcement gap that currently exists and maintain the integrity of capital controls while aligning legal certainty with India's gradual approach to liberalisation.

The ongoing rollout of the Digital Rupee needs to focus on caution and inclusion rather than speed.⁵³ It is important to eliminate or continue to have non-interest-bearing design features and have a limited amount that can be held in any wallet to protect commercial banks from rapid disintermediation or runs on digital currency. At the same time, expanding offline ₹ would enhance rural financial inclusion, provided good security and anti-fraud solutions are developed in parallel.⁵⁴ For public buy-in, the ₹ system should be aligned with the DPDPA, 2023, clarifying any obligations around data localisation, individual privacy, and the RBI's oversight. Ultimately, the credibility of any sovereign digital currency will rely as much on transparency and privacy as it will on its technical capabilities.

⁵² *ibid.*

⁵³ Economic Times, RBI Progressing Cautiously on Launch of Digital Currency: Governor Shaktikanta Das (11 February 2022) <https://economictimes.indiatimes.com/news/economy/policy/rbi-moving-cautiously-on-cbdc-wont-launch-in-haste-shaktikanta-das/articleshow/89478230.cms> accessed 6 November 2025.

⁵⁴ IBEF, RBIs Offline Digital Rupee is Here: Pay with ₹ Even Without Internet (14 October 2025) <<https://ibef.org/news/rbi-s-offline-digital-rupee-is-here-pay-with-e-even-without-internet#:~:text=also%20features%20offline%20payments%20using,expiry%20dates%2C%20geolocations%2C%20or%20merchant>> accessed 7 November 2025.

At last, Indias participation in the global regulatory environment will be instrumental in its digital currency strategy. Greater engagement in the IMF-FSB Data Gaps Initiative (DGI-3) will improve data quality around crypto flows and improve macroeconomic forecasting. In parallel, India should consider a pilot framework to pilot a regulated INR-stablecoin for cross-border settlements. This will allow for a digital alternative settled in rupees to lessen dollarisation pressure and ultimately achieve its vision of INR-internationalisation. Developing monetary models that embed digital currency adoption variables will prepare the RBI for liquidity and velocity changes as it develops its monetary policy instruments.⁵⁵

If India continues its current trajectory of combining fiscal deterrence, FEMA based control, and phased deployment of the Digital Rupee, its regulatory framework is likely to evolve into a two-tier system in which private digital assets remain tightly constrained as speculative instruments while the e₹ emerges as the primary state sanctioned digital medium of exchange. The success of this model will ultimately depend on whether the RBI can retain effective control over capital flows and monetary aggregates despite the parallel growth of offshore crypto markets.

⁵⁵ *RBI CBDC* (n 2).

ARTIFICIAL INTELLIGENCE AND DISABILITY RIGHTS: ENSURING EQUITY IN ACCESS AND DESIGN

—Aryan Raj & Shraddha Yadav*

ABSTRACT

Artificial intelligence has become a structural pillar that impacts the areas of education, workforce, health, and civic life. Although AI has empowerment opportunities among persons with disabilities, it also has dangers of exclusion. The idea of accessibility is entrenched both in law and in ethics as a legal and ethical requirements in international frameworks such as the United Nations Convention on the Rights of Persons with Disabilities, the Recommendation on the Ethics of Artificial Intelligence by UNESCO, or regional laws such as the European Accessibility Act. Market-based design perspectives, algorithmic bias and techno-solutionist rhetoric habitually undermine these practices, however; by introducing ableist assumptions into technologies that are purportedly neutral. In India, the most significant legal foundation of the accessible artificial intelligence is the Rights of Persons with Disabilities Act, 2016, which supplements the constitutional provisions of Articles 14, 21, and 41. Grass-root campaigns, including the projects funded by the AssisTech Foundation, and such projects as Mission AI Accessibility, show the use of AI in changing communication, education, and independence of people with disabilities. However, effective inclusion is still limited by poor mechanisms of enforcement, inadequacy of infrastructures preparation, and overreliance on voluntary adherence. This article argues that in addition to the law, the achievement of fair access to artificial intelligence would require enforceable standards, strong ethical responsibility, and participatory design paradigm that makes people with disabilities co-creators. It is only with the adoption of these systemic mitigation efforts that AI can become the driver of justice, dignity, and inclusivity.

Keywords: *Artificial Intelligence, Accessibility, Disability Inclusion, Assistive Technology, Algorithmic Ethics.*

* The authors are students at National University of Study and Research in Law, Ranchi

I. INTRODUCTION

In contemporary society, artificial intelligence is becoming an increasing pervasive force which is shaping various aspects of everyday life. It is impacting professional lives, education system, mode of communication and even, social interactions. It is no longer confined to use by professionals and experts. Although the AI revolution has the potential to greatly benefit individuals with disabilities by removing obstacles to inclusion, there is also a risk of greater inequality and social exclusion as artificial intelligence advances. Algorithms used by artificial intelligence are typically developed by individuals without disabilities. Voice assistants and visual aids, for instance, are designed to help, but they frequently assume that all users are “normal” in the same sense, for instance, speaking clearly or having eyesight. Thus, these people with a range of abilities feel excluded. This has highlighted the main argument that artificial intelligence is not a neutral tool, instead, its functionality is controlled by the decisions and algorithms created by the people who develop it, which often cause bias against people with disabilities.

This problem is not about a simple technological concern, but an issue of rights and equality. Accessibility is elucidated by the United Nations Convention of Rights of Persons with Disabilities as a right but not charity. European Union laws are also based on accessibility that is conditional on protection. However, despite the explicit directions on the international and regional levels, these are irregularly enforced. Commercial organizations are often not very concerned about universal access, thus making the issue of AI accessibility a legal and not a moral or ethical issue. In this regard, the conversation about the AI access makes it possible to critically explore the notions of fairness and respect and equal justice in an ever more digital society.

These tensions are more pronounced and obvious in the Indian environment. The accessibility of technology is provided with a very solid legal framework by the Indian Constitution and the Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 2016. Courts have also continuously stated an implication of the availability of online services as an indispensable fraction of the right to life and equality. Players in the civil society in India have driven substantive development of inclusive technology, such as the AssisTech Foundation, and state efforts, including Digital India and national policies on artificial intelligence. Still, infrastructural shortages, disproportionate implementation, and the existence of demonstrative prototypes still smother the underlying concepts of access which support extensive use. The 2025 event, AI to Empower Persons with Disabilities, highlighted a

fundamental tension between the transformative potential of advanced and open-source AI systems and the persistent structural barriers that hinder the realisation of constitutional guarantees of accessibility.

The current article provides a critical analysis of how India is involved in the pragmatic and constitutional approach to artificial intelligence and foreshadows the ethical dilemmas associated with designing algorithms and the position of AI in the context of the human-rights discourse. It argues that fair use of artificial intelligence cannot be ensured by any means of market forces or corporate innovation programs only. Rather than being a passive recipient of the digital future, accessibility must be based on strong ethical commitments, legally binding standards, and participatory design processes that recognize people with disabilities as co-creators.

This article is structured in the following manner- Section II explores how artificial intelligence is being developed in the international framework of human rights, including international and regional laws like the United Nations Convention on the Rights of Persons with Disabilities, the UNESCO Recommendation on the Ethics of Artificial Intelligence, and comparative models in the United States and European Union. Section III examines the essential ethical issues associated with the accessibility of AI, such as algorithmic bias, the opposition between commercial innovation and universal design, and the data privacy representation paradox. Section IV appraises the Indian constitutional and statutory framework of accessibility with specific reference to judicial developments, the Rights of Persons with Disabilities Act, 2016, and the current state and private efforts in AI- driven inclusion. Section V suggests the novel solutions for the highlighted issues. While, Part VI wraps up with a conclusion.

II. ARTIFICIAL INTELLIGENCE AND THE GLOBAL HUMAN RIGHTS DISCOURSE

Significant concerns have been raised under the framework of global human rights in relation to accessibility for people with disabilities due to the increasing reliance on the artificial intelligence. This issue is most prominently addressed by the United Nations Convention on the Rights of Persons with Disabilities (CRPD), which establishes binding obligations on States to ensure equal access to information and communication technologies.

While Article 21 of the CRPD¹ provides freedom of expression and access to information, including through accessible formats and technologies, Article 9² requires States Parties to provide equitable access to information and communication technology. These provisions, read together, establish a clear human rights obligation to design, regulate, and deploy AI in ways that are accessible to disabled individuals. The United Nations has reinforced this interpretation through the Disability Inclusion Strategy, 2019,³ which commits all UN entities to integrate accessibility and inclusion standards in the use of emerging technologies, including AI. This approach signifies that availability is not a charitable concession but a component structural necessity that forms the governance.

UNESCO is also developing the template of the global system with its Recommendation on the Ethics of Artificial Intelligence, 2021,⁴ the first international standard-setting instrument on AI. The Recommendation emphasizes inclusivity, fairness, and human dignity, and specifically, the states are required to facilitate human access to AI systems by persons with disabilities. This awareness is essential, because much of the AI systems, be it voice assistants, facial recognition systems, generative iterations, or others, incorporate an assumed default user who might be discriminatory. In turn, the Recommendation transforms the slogan of the disability-rights movement- “nothing about us without us”, into a set of global standards of norms.

Regional legal frameworks complement these commitments. In the United States, the Americans with Disabilities Act⁵ has been interpreted to extend to digital and AI-enabled environments. Courts have held that private actors offering goods and services must ensure accessibility. In *Gil v Winn-Dixie Stores*,⁶ a visually impaired plaintiff who relied on screen-reader software sued under Title III of the ADA, arguing that Winn-Dixie’s inaccessible website denied him equal access. The Eleventh Circuit acknowledged that barriers to digital services could amount to a concrete injury under Article III standing. The court observed that there is no doubt that a commendable purpose of the ADA is to enhance the lives of Americans with disabilities. We also recognize that for many Americans like Gil, inaccessibility online

¹ Convention on the Rights of Persons with Disabilities (adopted 13 December 2006, entered into force 8 May 2008) A/RES/61/106 (CRPD) art 21.

² Ibid, art 9.

³ United Nations, United Nations Disability Inclusion Strategy, 2019, <https://www.un.org/en/content/disabilitystrategy/assets/documentation/UN_Disability_Inclusion_Strategy_english.pdf> accessed 10 April 2026.

⁴ UNESCO, ‘Recommendation on the Ethics of Artificial Intelligence’ (23 November 2021) UNESCO Doc SHS/BIO/AHEG-AI/2021/1.

⁵ Americans with Disabilities Act 1990, 42 USC §§ 12101–12213.

⁶ *Gil v Winn-Dixie Stores Inc* 993 F3d 1266, 1270 (11th Cir 2021).

can be a significant inconvenience. But the court did not give judgement in Gil's favour as websites are not considered as the place of public accommodation.

In the European Union, the European Accessibility Act, 2019 imposes accessibility standards on digital products and services, including e-commerce and e-books, and its logic is readily extendable to AI applications.⁷ The EU's Artificial Intelligence Act, which reached political agreement in 2023, introduces a risk-based classification, treating AI in employment, education, and essential services as "high-risk" systems requiring stringent safeguards.⁸ Accessibility considerations are embedded in this framework, ensuring that persons with disabilities are not disproportionately disadvantaged by high-risk AI systems. Moreover, the EU's General Data Protection Regulation (GDPR) continues to influence the global debate, particularly around data protection for vulnerable groups.⁹ The principles of data minimisation and purpose, as defined in the GDPR, should be seen as empowerment tools and not privacy formalities for people with disabilities, whose health and biometric data are most of the time handled by artificial intelligence.

These regional and global frameworks can be seen as a decisive move toward the institutionalisation of accessibility as a norm of law and the expansive spread of artificial intelligence as they emphasize inclusivity in technical regulation by creating a normative order. Although these tools have a strong legal basis, they also highlight the need to have cross-sectoral collaborations and enforcement measures in such a way that the legal constructs can be realised in the lived reality. In this connection, the question of whether the international human-rights regime has the capacity to truly shift the direction in the development and use of technologies, thus making the provision of AI little more than a strictly technical matter, approaches the forefront of the issue.

Although the international and regional main frameworks mentioned above provide a solid legal basis for the accessibility of artificial intelligence systems, they also highlight that converting the written commitments into actual experiences is still a big challenge. The fact that exclusion happens even when the law has been formally guaranteed suggests that the issue of AI accessibility may not be fully grasped by looking at law only. This calls for a discussion

⁷ Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services [2019] OJ L 151/70.

⁸ Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 168/1].

⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L 119/1.

about the ethics of AI design and use, especially the deeply held ones, biases, and structural priorities which define the development of technology.

III. ETHICAL CHALLENGES OF AI ACCESSIBILITY

Accessibility is a legal requirement and is contemplated by both regional and international systems, although legislation is not enough to solve the underlying problems that are presented by AI. Through personal experience shared by persons with disabilities, there are empirical proofs showing that both omissions in regulations and beliefs and assumptions on the part of technology are the barriers to access, which cause disabilities. Put differently, the moral effects of the AI availability also presuppose that there will be a thorough consideration of whose bodies, voices, and experience affect technological systems; that is not just a matter of compliance. Although it could be transformative, the artificial intelligence does often tend to reflect the economic and social frameworks of the societies where it is created, and persons with disabilities, who had always been marginalised in policy and innovation, are particularly likely to be left out when the potential benefits of the system are overshadowed by market driven priorities.

A. Problem of Algorithmic Bias

One of the main difficulties is the problem of algorithmic bias, which is not only caused by biased data sets but also compensatory rules carried within the design. In 2017, scientists proved that AI-based recruitment apps systematically reduced the score of resumes with disability-related associations, even in cases where the qualifications were not different.¹⁰ The harm caused by it is twofold: it prevents a person with disability from participating in the economy and justifies the ableist stereotypes under the banner of algorithmic unbiasedness. The same can be said about generative AI systems, which often cast people with disabilities as inactive or pitiful individuals, thus, entrenching the dependency tropes over the agency tropes.¹¹ These outputs involve the manner in which data on the training that is based on a world permeated with inequality is bound to encode and replicate the same inequalities.

B. Conflict between commercial innovation and universal design

The other ethical controversy is the conflict that exists between commercial innovation and universal design. The principle of universal design, which is embedded in the disability-rights

¹⁰ Pauline T Kim, 'Data-Driven Discrimination at Work' (2017) 58 William & Mary Law Review 857, 879–81.

¹¹ Abeba Birhane and others, 'The Dangers of Stochastic Parrots: Bias and Stereotypes in Large Language Models' (2022) Proceedings of the ACM Conference on Fairness, Accountability, and Transparency Abeba.

discourse, holds that technologies must be designed to be universally usable without the need to retrofit but in reality, the corporations often consider accessibility as the perfunctory aspect, which they will incorporate only after profitability is ensured.¹² This approach shifts the ethical burden onto disabled users, who must continually advocate for recognition. In India, for example, the government's flagship "Digital India" program has expanded mobile and internet penetration, but accessibility guidelines issued under the Rights of Persons with Disabilities Act, 2016 remain weakly enforced.¹³ Many state e-governance portals are incompatible with screen readers, and even Aadhaar authentication systems often fail for persons with visual or motor impairments, creating barriers to accessing welfare schemes that are, in theory, rights-based entitlements.¹⁴ The ethical stakes are stark as without inclusive design, AI-enhanced governance risks hard-coding exclusion into the very architecture of citizenship.

C. Protection of privacy versus need for representation

Ethical discourse around AI also confronts a data paradox which is the protection of privacy versus the need for representation. The European General Data Protection Regulation¹⁵ coupled with similar laws in India, have reinforced the need to reduce collation of personal information, which is sensitive including health and disability status.¹⁶ However, there is no such data available, and this hampered the ability to develop an algorithm that could identify or support people with disabilities. This lack of disability-sensitive data collections hinders invisibility, whereas collection creates the risk of misuse, surveillance or stigmatization. As a result, policy makers have to be able to balance conflicting moral requirements the right to privacy and the right to inclusion.

D. Inaccessible Environments in AI Systems

Another problem of techno-solutionism is the belief that disability can be fixed with the help of artificial intelligence. Exoskeletons, brain-computer interfaces, and AI-enhanced prosthetics happen to be widely praised as innovative, however, they narrow the scope of disability by positioning it as an individual malfunction to be remedied rather than a social interaction posed by inaccessible environments.¹⁷ The disability activists argue that this orientation negatively

¹² Ronald L Mace, 'Universal Design: Barrier-Free Environments for Everyone' (1985) 33(1) Designers West

¹³ Rights of Persons with Disabilities Act 2016.

¹⁴ Nidhi Singal and Shilpi Banerjee, 'Digital Exclusion: Disabled Citizens and India's Aadhaar System' (2021) 17 Disability & Society 1123, 1125–28.

¹⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L 119/1.

¹⁶ Digital Personal Data Protection Act 2023.

¹⁷ Alison Kafer, *Feminist, Queer, Crip* (Indiana University Press 2013) 45–47.

commercialises the bodies of the disabled and excludes systemic change efforts, like inclusive education or workplace access, which are expensive though, but more revolutionary.¹⁸

These ethical dilemmas are aggravated by global digital divide. The concentration of AI systems is found in the Global North, but implementation is becoming more critical in the Global South, where the problem of infrastructural inequalities exacerbates the issue of accessibility. An example is that most disabled users in multilingual countries like India are not only excluded but also not catered to due to the fact that most speech-recognition algorithms are usually trained on American English languages and therefore cannot understand accented speech.¹⁹ Here, colonialism background and ethics build up, where the electronic structures built in the other areas unleash cultural and linguistic standards that rollout the native communications patterns.

The control over such challenges is disjointed. Even international instruments, including the Recommendation on the Ethics of AI by UNESCO, are guided by the principles of fairness and inclusiveness, but being non-binding makes them hard to transform. Corporate codes of AI ethics multiply, but they are often PR actions, lacking adequate accountability in situations where damage is inflicted. According to scholars, the principle of “nothing about us without us” should be operationalised as an ethical imperative and that requires persons with disabilities, to be not just consulted but become co-designers and decision-makers in AI regulation.²⁰ The accessibility will be subject to the market logics and political oversights until such actions are taken.

The problem of the accessibility of AI is not on the margins of its ethical issues but at the very heart of the justification of AI as a social project. They require an accounting to values that we invest in our most effective technologies, whether our values are those that are more focused on efficiency and profit or justice and dignity. To overcome this situation, ethical reflections should not remain an aspirational explanation, but be transformed into enforceable guidelines that can view accessibility as an entitlement, but not charitable activity.

¹⁸ Sins Invalid, *Skin, Tooth, and Bone: The Basis of Movement is Our People* (2nd edn, Sins Invalid 2019) 13–15.

¹⁹ Emily M Bender, ‘Rule #2: Respect the Subjective Experiences of Language Users’ (2021) 37 *Computational Linguistics* 699, 702–04.

²⁰ Tom Shakespeare, *Disability Rights and Wrongs* (2nd edn, Routledge 2014) 182–84.

IV. INDIAN CONSTITUTIONAL FRAMEWORK AND THE REALITY OF ACCESSIBLE AI

A. Constitutional and Statutory Framework

India has positioned itself in an emerging centre of artificial intelligence research, not only commercial but also uses applications of public interest, of which disability inclusion is becoming more pronounced. Countless governmental initiatives as well as independent ones introduce AI as a tool of accessibility. For instance, in 2025 the Department of Empowerment of Persons with Disabilities (DEPwD) collaborated with NITI Aayog to release a program called Mission AI Accessibility, which was announced at the conference AI for Empowering PwDs in Bengaluru. The initiative announced the development of a National Disability Support AI Chatbot, designed to help persons with disabilities navigate welfare entitlements and grievance redressal, and showcased pilot projects in AI-powered assistive devices ranging from real-time captioning platforms to smart goggles for blind users that recognize faces and detect objects in real time.²¹ Similar innovation is visible in the private sector: start-ups supported by the AssisTech Foundation (ATF) have developed AI-based screen readers, voice-enabled payment systems, and adaptive learning platforms that expand autonomy for persons with visual and cognitive impairments.²² A particularly promising development has been the emergence of AI-based assistive applications for children with disabilities in India. Tools like AACDD and DYSXA address learning barriers faced by children with dyslexia and dysgraphia through animations, interactive quizzes, and multi-sensory approaches to reading and spelling. Applications such as VAANI and Dhvani focus on speech and hearing impairments, the former enabling communication through voice recognition and the latter offering speech-to-text conversion for deaf users. While programs like DAAD (Digital Arts Academy for the Deaf) offer hybrid IT courses with Indian Sign Language and subtitles, increasing career opportunities for deaf learners, government-backed platforms like I-STEM go beyond classrooms by offering inclusive academic resources, collaborative innovation spaces, and accessible research tools. Collectively, the initiatives described show that AI can be used to promote inclusiveness at its very beginning, incorporating accessibility into professional

²¹ Department of Empowerment of Persons with Disabilities (DEPwD), 'DEPwD Unveils AI-Powered Platforms to Deliver Scholarships, Healthcare and Livelihood Support to Differently Abled' (30 May 2025) Economic Times Government <<https://government.economictimes.indiatimes.com/news/governance/india-launches-ai-innovations-to-support-differently-abled-citizens/121528943>> accessed 10 April 2026.

²² AssisTech Foundation, 'AssisTech Foundation (ATF) Welcomes 10 Assistive Technology Start-Ups to ATF Enable Acceleration Program Cohort 5' (1 February 2023) <IndianWeb2, <https://www.indianweb2.com/2023/02/assistech-foundation-atf-welcomes-10.html>> accessed 10 April 2026.

development, education, and welfare programmes. According to these efforts, India has started paying more attention to accessibility in its AI ecosystem because inclusive technical design can be both a competitive edge and a constitutional duty.

The constitutional structure provides a good platform to this change. Article 14 ensures the equality before law²³ and Article 21²⁴ enlarges the right to life and dignity in a broad, purposive context that has always been used by courts to mean access to the digital and involvement in the lives of society. The Directive Principles, in Article 41,²⁵ also teach the State to protect the right to work, education and public assistance in instances where the citizens are disabled. All those provisions comply with the fact that accessibility is not a matter of mercy. These constitution commitments have been interpreted on several occasions by the Supreme Court in a broad manner. In *Justice Sunada Bhandare Foundation v Union of India*, the Court reprimanded the government on the ground that it did not adopt any disability-rights laws and emphasized that the concepts of accessibility and equal participation were two of the building blocks of the Article 21 promise of dignity.²⁶

More recently, in 2025, in case of *Amar Jain v Union of India & Ors*, the Court explicitly recognized digital access as part of the right to life, holding that state portals and online services must comply with Section 46 of the Rights of Persons with Disabilities Act, 2016.²⁷ The court issued several directions to make the KYC process more accessible for persons with disabilities.

The RPwD Act represents India's most ambitious statutory attempt to implement these commitments. The Act is designed based on the United Nations Convention of the Rights of Persons with Disabilities, which India ratified in 2007 and provides that the information and communication technologies must be accessible and that the government should adopt the standards that are harmonised with the international standards. The government has proposed IS-17802 in 2023, as part of Rule 15 of the Act, matching the guidelines to accessibility standards in the world, including the WCAG 2.1 and EN 301: 549.²⁸ That action was an indication of an effort to codify abstract promises into formal design requirements.

B. Implementation, Enforcement, and Civil Society Challenges

²³ Constitution of India 1950, art 14.

²⁴ Constitution of India 1950, art 21.

²⁵ Constitution of India 1950, art 41.

²⁶ *Justice Sunanda Bhandare Foundation v Union of India* AIR 2014 SC 2869.

²⁷ Rights of Persons with Disabilities Act 2016, s 46.

²⁸ Ministry of Social Justice and Empowerment, Rights of Persons with Disabilities (Amendment) Rules 2023 – Accessibility Standards on ICT Products and Services (Government of India, 10 May 2023).

However, there is still an uneven implementation. In 2024, just 95 sites of the central-government were found to be visible to screen-readers, the same number as in 2020 despite legal requirements.²⁹ Likewise, Aadhaar-based system of authentication, which is needed to receive welfare programs, does not work regularly with persons with motor or visual disabilities, hence disqualifying them in the benefits to which they have a legitimate right.³⁰

Though the flagship state initiative on e-governance, the Digital India, has been successful in increasing the spread of broadband and e-government portals, it has not always incorporated accessibility in its implementation strategy. Researchers note that RPwD Act accessibility regulations are poorly implemented, and most current compliance is not taken by the state but by the courts.³¹ For example, in the case of *National Association of the Deaf v Union of India*, the Delhi High Court ordered the authorities to provide sign language interpretation of official broadcasts, considering accessibility as part of the equality under Article 14.³² These instances can teach that even though there are constitutional and statutory undertakings, they usually need a judicial push to become real-life solutions.

The Indian experience with AI accessibility is also shaped by tensions between innovation and structural inequality. At one end, elite conferences in Bengaluru celebrate AI-enabled prosthetics, exoskeletons, and biomedical devices. At the other, millions of PwDs still lack access to basic screen reader-friendly e-governance portals or affordable assistive software. Disability rights advocates argue that this reflects a techno-solutionist bias, where glamorous prototypes attract attention and funding, while mundane but vital accessibility features, captioning in regional languages, interoperable payment apps for blind users, or reliable voice recognition for accented Indian English, remain under-prioritized. A 2023 study found that Indian speech recognition systems misinterpret over 30% of inputs from speakers with dysarthria or stammering, underscoring the systemic mismatch between AI design and linguistic diversity.³³

²⁹ Masoom Reza, 'Why Does India Fail to Address Digital Accessibility Gaps?' (6 September 2024) Newslaundry, <<https://www.newslaundry.com/2024/09/06/why-does-india-fail-to-address-digital-accessibility-gaps>> accessed 10 April 2026.

³⁰ Nisha Nambiar, 'Activists Demand Alternative Aadhaar Authentication Methods to Stop Benefits Denial' (15 August 2025) Times of India <<https://timesofindia.indiatimes.com/city/pune/activists-demand-alternative-aadhaar-authentication-methods-to-stop-benefits-denial/articleshow/123462163.cms>> accessed 10 April 2026.

³¹ Syeda Tahseen Kulsum, K Madan Gopal, Arpita Aggarwal and Prasanth KS, 'Assessment of the Rights of Persons with Disabilities Act, 2016 in India: A Comprehensive Study on Implementation and Impact' (2024) 6 International Journal for Multidisciplinary Research.

³² *National Association of Deaf v Union of India* 2011 SCC OnLine Del 4954.

³³ A Gupta, R Kumar and Y Kumar, 'An Automatic Speech Recognition System in Indian and Foreign Languages: A State-of-the-Art Review Analysis' (2023) 17(2) Intelligent Decision Technologies 505–526, <<https://doi.org/10.3233/IDT-220228>> accessed 10 April 2026.

Civil society and non-state actors play a vital role in bridging these gaps. The AssisTech Foundation has incubated over fifty start-ups dedicated to accessible technology, but most remain dependent on philanthropic grants and lack pathways to integrate into mainstream corporate ecosystems. International comparisons further emphasize India's deficit. Ambition and responsibility are out of balance because Indian regulatory frameworks rely on voluntary compliance, whereas the European Accessibility Act places legal obligations on digital businesses. A major difference between the two is that Indian regulatory systems mostly depend on voluntary compliance and the availability of advisory standards for accessibility such as the Rights of Persons with Disabilities Act, 2016 and IS-17802 guidelines. On the other hand, the European Accessibility Act, 2019 authorizes the imposition of binding legal obligations on economic operators, resulting in digital products and services that must meet enforceable accessibility requirements within the EU market. This difference is quite critical since the EAA places accessibility as a statutory obligation rather than a mere policy goal, and it introduces market surveillance and penalties for non-compliance. India, on the other hand, still mainly relies on judicial enforcement and fragmented implementation by the executive, which leads to uneven compliance in both public and private digital platforms. Therefore, in order to reach the same level, India should shift to mandatory accessibility certification, statutory punishment for non-compliant digital services, and the incorporation of accessibility requirements directly into the sectoral regulation that governs AI systems. As a result, due to voluntary compliance, creators may treat accessibility as a choice rather than a human right. Overall, India's journey of the development of AI and regulatory frameworks reflect a paradox. On one hand, there is strong emphasis on making AI accessible through the judicial decisions, constitutional provisions, the RPwD act, and the growing startups, but, on the other hand, due to infrastructural deficiency, inadequate enforcement and cultural biases, thousands of people still lack equal access to the AI. This problem will not be resolved until the AI projects will not be made with the view of observing accessibility as a structural necessity rather than a later and optional choice.

V. INSTITUTIONAL AND REGULATORY FRAMEWORK FOR ACCESSIBLE AI

Although the above discussion shows that accessibility in the field of artificial intelligence is considered as an established concept in both international and domestic systems, a wide disparity exists between the normative commitments and enforceable obligations. In order to

bridge this gap, the following institutionally specific and legally oriented suggestions are offered.

To begin with, an obligatory pre- deployment AI accessibility audit system needs to be established according to the Rights of Persons with Disabilities Act, 2016. This mechanism ought to mandate that all AI systems, especially those used in governance, employment, education and financial services, be audited regarding accessibility by an independent entity before implementation. There should be a regulatory body with the mandate to certify compliance, penalise non-compliance and suspend the inaccessible systems, e.g, the Office of the Chief Commissioner for Persons with Disabilities or a specialised AI Accessibility Board. This would make the issue of accessibility more of a legal requirement rather than a post hoc requirement.

Second, AI governance structures need to have statutory representation of persons with disabilities. This can be done by the legal requirement of quotas in the national AI advisory committees, ethics committees and standard-setting bodies like the ones engaged in the development of IS-17802. This type of representation cannot be consultative but decision-making. Incorporating the principle of nothing about us without us into statutory rules would change the perception of accessibility being a marginal issue to a design imperative.

Third, it must be declared in the Indian constitutional jurisprudence that the inaccessibility of AI is a constitutional tort that can be resolved in the light of Articles 14 and 21. Courts ought to allow people to directly question non-accessible digital infrastructures, especially those that are operated by the state, as a breach on the right to equality and dignity. This would facilitate granting of compensation, structural remedies and sustained mandamus as a guarantee to conformity. This would bring digital accessibility to the same level of protection of constitutional shields against systemic exclusion.

Fourth, accessibility standards like IS-17802 must be judicially enforceable as opposed to being aspirational directives. The non-adherence to such standards should be considered by courts as the breach of statutory obligations due to the Rights of Persons with Disabilities Act, 2016, which can be abolished under the writ jurisdiction and contempt cases. This would resolve the long-standing issue of poor implementation and make technical standards legally binding.

These suggestions are unlike the current strategies of focusing on voluntary standards and ethical appeals and seek to enforce legal obligations, institutional responsibilities, and participatory governance. The problems that have been discussed in the previous Parts, i.e., the limited implementation of the norms of accessibility, the lack of involvement of the persons

with disabilities into AI engineering procedures and the lack of legal responsibility, require specific institutional and legal measures.

VI. CONCLUSION

The availability of artificial intelligence to individuals with disabilities indicates a basic conflict at the interface of technology, law, and human rights. Although legal frameworks like the CRPD and regional legal regimes have solidly enshrined accessibility as a legal duty, and not a charity, there is little practical effect due to weak enforcement, design priorities in the market, and structural inequalities. As this paper has revealed, AI is not a neutral technology; it is a mirror and replica of the biases that exist in the social and institutional environments, in which it is created.

The Indian experience summarizes the potential and constraints of reconciling artificial intelligence with constitutional values. The strong normative basis of inclusive technological development has been established with the help of Articles 14, 21 and 41 of the Constitution, which are interpreted in the light of the Rights of Persons with Disabilities Act, 2016. The rights have also been extended with judicial interventions to encompass digital accessibility. Nevertheless, the existence of unreachable digital infrastructures, discrepancy in application of statutory standards and excessive dependence on voluntary adherence points to a large discrepancy between legal promises and lived experiences.

This paper has maintained that incremental reform is not the answer to close this gap. The concept of accessibility needs to be redefined as a structural and enforceable part of AI governance, as opposed to an afterthought or a corporate privilege. The proposals developed in this article aim to go beyond the current frameworks by integrating accessibility into both regulatory design and constitutional implementation and participatory decision-making.

Finally, it is not whether artificial intelligence can be made accessible but whether legal and institutional systems are ready to make and enforce the accessibility as a right issue. The future of AI will not just be characterized by its technological advancement but also by its ability to promote equality, dignity, and inclusion. To achieve the transformative potential of artificial intelligence in a just and equitable society, it is necessary that persons with disabilities be seen as co-creators, and not passive receivers, of technological systems.

LIABILITY AND ACCOUNTABILITY IN AI-DRIVEN HEALTHCARE: NAVIGATING ETHICAL AND LEGAL CHALLENGES IN MEDICAL MISHAPS

—Kavya Pradeep and Jayanth Siva*

ABSTRACT

*The growing use of artificial intelligence (AI) in medical care has had a significant impact on the diagnostic and clinical decision-making process. AI-inspired healthcare, has demonstrated unanswered ethical and legal issues related to liability and responsibility of medical errors. In contrast to conventional medical technologies, AI systems have the ability to independently impact clinical outcomes, thus disrupting the established beliefs of human control and responsibility when making medical decisions. The ethics and legal implications of the concept of liability in AI-inspired healthcare, namely the Indian legal and regulatory landscape, are critically discussed in the paper. The article posits that current negligence paradigms do not adequately reflect the distributed relationship inherent in AI-assisted medical practice. Although AI systems are not a legal person, and cannot be directly held responsible, liability is disproportionately placed on clinicians as the final legal decision-makers when it comes to algorithms, although they do not control their creation, training data, and update procedures. Relying on judicial precedents of India like in *Jacob Mathew v. State of Punjab*¹ and *Kusum Sharma v Batra Hospitals*², the article shows how the conventional standards of care are doctrinally problematic when used in the context of clinical decisions made with AI involvement. It also examines the fragmented regulatory approach used in India including the Medical Devices Rules of 2017, the Consumer Protection Act of 2019, Digital Personal Data Protection Act 2023 and the Information Technology Act of 2000, placing it in the context of similar trends in other countries such as the Artificial Intelligence Act adopted by the European Union and the United States Software as a Medical Device model. It concludes the existing regulatory paradigms focus on safety, ethics, and compliance and lack many provisions on liability in case of medical damage caused by AI.*

* The authors are students at Tamil Nadu National Law University (TNNLU).

¹ *Jacob Mathew v State of Punjab* (2005) 6 SCC 1.

² *Kusum Sharma v Batra Hospital and Medical Research Centre* (2010) 3 SCC 480.

Keywords: *Artificial Intelligence, Medical Liability, Consumer Protection Act 2019, Information Technology Act 2000, Medical Devices Rules 2017, Digital Personal Data Protection Act 2023, Clinical Decision-Making, Distributed Responsibility.*

I. INTRODUCTION

The integration of AI into the clinical domain represents a fundamental change in the patient-physician relationship and the traditional structures of medical accountability. Historically, the practice of medicine has been governed by a direct relationship between a human professional and a human patient with technology used as a passive instrument under direct control of the physician. However, with rapid technological developments, the introduction of a “*third agent*” characterized by opacity, adaptability and a degree of agency that challenges existing ethical and legal doctrines.³ As healthcare systems worldwide, particularly in India transition towards the “*AI for All*” vision the challenge lies in ensuring innovation does not outpace the development for ethical safeguards.⁴

The article argues that the existing legal regulatory framework governing AI-assisted medical practice in India is structurally inadequate to address the novel accountability challenges posed by autonomous AI systems. The current negligence doctrine, which concentrates liability on the clinician as the proximate human decision maker and fails to reflect the distributed and opaque nature of AI mediated harm. It is further contended that a coherent response requires not merely the incremental adaption of existing doctrines but a principled reconceptualization of responsibility that acknowledges the contributions of developers, institutions and clinicians in proportion to their actual control over AI systems.

II. ETHICAL FOUNDATIONS AND LIABILITY FRAMEWORKS IN AI-DRIVEN HEALTHCARE

The integration of AI into healthcare has fundamentally reshaped both the ethical foundations of medical practice and the frameworks through which liability is understood. While traditional bioethics are grounded in autonomy, beneficence, non-maleficence and justice, which continue to provide a normative baseline, the rise of AI driven decision making introduces complexities

³ Tuan Pham, ‘Ethical and Legal Considerations in Healthcare AI: Innovation and Policy for Safe and Fair Use’ (2025) 12(5) Royal Society Open Science 241873.

⁴ Clara Cestonaro and others, ‘Defining Medical Liability When Artificial Intelligence Is Applied to Diagnostic Algorithms: A Systematic Review’ (2023) 10 Frontiers in Medicine.

that these principles were not originally designed to address. The opacity of algorithmic systems, the redistribution of clinical authority between human and machine and the emergence of systemic rather than individual harms necessitate a re-evaluation of ethical obligations alongside corresponding legal accountability structures.

A. The Shift in Bioethical Principles

The traditional framework of bioethics primarily articulated through the four pillars of autonomy, beneficence, non-maleficence and justice, remains the essential starting point for any ethical evaluation of technology in medicine⁵. Scholars have proposed a fifth essential pillar that is explicability (referred to as transparency or accountability) which requires that AI systems be interpretable, their decisions be traceable and their developers and deployers answerable to outcomes. This principle addresses the unique epistemological challenges posed by autonomous AI systems in clinical contexts.⁶

1. Reinterpreting Autonomy and the Crisis of Agency

In the context of AI, this principle is under threat from information asymmetry created by complex algorithms.⁷ Respect for autonomy emphasizes the right of individuals to make informed decisions about their own healthcare. Yet when a physician utilizes a deep-learning model to recommend treatment, the rationale is often hidden within thousands of processing layers.⁸ If the physician cannot explain ‘why’ the AI arrived at a specific conclusion the patient’s ability to exercise true autonomy is compromised and their consent is thereafter based on an opaque process rather than a traditional medical rationale. Furthermore, automation bias, which is the human tendency to defer to an automated system erodes professional agency⁹ creating a moral buffer, a form of psychological distancing where clinicians may ignore their own expertise in favour of a statistically generated output¹⁰ where it also argued that this dynamic effectively delegates moral authority to a machine that lacks moral agency however, it must be noted that this characterisation remains philosophically contested and not all ethicists agree that deference to a probabilistic output constitutes a formal delegation of moral authority.

⁵ Edmond & Lily Safra Center for Ethics, Harvard University, ‘How Bioethics Can Inform Ethical AI Governance’ (15 March 2024).

⁶ Ahmad A Abujaber and Abdulqadir J Nashwan, ‘Ethical Framework for Artificial Intelligence in Healthcare Research: A Path to Integrity’ (2024) 14(3) World Journal of Methodology 71–94.

⁷ Shambhavi Naik and Bharath Reddy, ‘A Framework for the Governance of AI in Healthcare for India: An Exploratory Model’ (2025) Indian Journal of Medical Ethics (8 May 2025).

⁸ L S Hjort, ‘Informed Consent to AI-Based Decisions in Healthcare: Must Patients Understand the AI’s Output?’ (2025) 11 Oslo Law Review 1–21.

⁹ Alberto Giubilini, ‘It Is Not About AI, It’s About Humans: Responsibility Gaps and Medical AI’ (2025) 22(3) Journal of Bioethical Inquiry 527–537.

¹⁰ *ibid.*

2. Beneficence and Non-Maleficence

The ethical mandate of beneficence (doing good) requires AI systems to maximize human well-being and solve societal challenges such as resource scarcity. Models that are AI-driven have shown the ability to predict gradings from brain MRIs with precision that exceeds human experts however, the principle of non-maleficence (the duty to avoid harm) serves as a critical check on such developments. Such flawed training can produce two distinct categories of harm, first unintentional harm where erroneous outputs cause adverse clinical outcomes without any deliberate intent and second, deliberate misuse where datasets are intentionally manipulated to produce biased or false clinical results.¹¹ The ethical responsibility shifts to developers and institutes to ensure models undergo rigorous pre-deployment testing to prevent errors like the 23% higher false-negative rate for pneumonia detection found in rural populations.¹²

B. The Responsibility Gap

The most profound ethical challenge is the responsibility gap where an adverse outcome occurs, yet no individual agent can be held fully responsible due to the autonomous nature of AI. As machines learn beyond initial programming, the black box nature of algorithms means the epistemic condition is the requirement that an agent knows what they are doing and its consequences cannot be fully met by human operators.¹³ The moral crumple zone describes how a responsibility for a system-level failure is often misattributed to the nearest human operator.¹⁴ In automated surgical environments the surgeon may become a liability sponge bearing legal consequences for the software glitches they had no power to prevent thereby effectively shielding the technological system at the human operator's expense.¹⁵ Under the Indian tort law, the absence of a clearly identifiable human tortfeasor creates considerable difficulty in establishing causation and duty. The nearest analogous framework would be vicarious liability that proves inadequate where harm flows from algorithmic processes rather than from a human agent's act or omission. Courts applying the standards in *Kusum Sharma v*

¹¹ Yue Li and others, 'Reducing Misdiagnosis in AI-Driven Medical Diagnostics: A Multidimensional Framework for Technical, Ethical, and Policy Solutions' (2025) 12 *Frontiers in Medicine* 1594450.

¹² M B Bagwan, Tanya Joshi and Rahul Atul Goswami, 'Liability in Robotic Surgery: Legal Frameworks and Case Studies' (2025) 14(2S) *Journal of Neonatal Surgery* 70–77.

¹³ *ibid.*

¹⁴ Dinesh Kumar and others, 'Distributing Ethical Responsibility in Hybrid Human–AI Systems: A Conceptual Framework and Evaluation Model' (2025) *Journal of Information, Communication & Ethics in Society* 1–18. 'The Bolam Test: A Seismic Change in the Hon'ble Supreme Court's Stand on Its Acceptability' (2022) 44(3) *Journal of Indian Academy of Forensic Medicine* 2–6.

¹⁵ Madeleine Clare Elish, 'Moral Crumple Zones: Cautionary Tales in Human–Robot Interaction' (2019) *Engaging Science, Technology, and Society*.

Batra Hospitals will find that the conventional inquiry into whether the treating professional exercised reasonable care is insufficient when the professional's decision was substantially shaped by an opaque autonomous system. Meaningful accountability requires a structural legal response not merely the designation of a human responsible person by default.¹⁶

II. THE BOLAM AND BOLITHO STANDARDS IN THE AI ERA AND OTHER CASES

In India, the standard of care is historically defined by the Bolam Test from the case *Bolam v Friern Hospital Management Committee* which states that a doctor is not negligent if their actions align with a responsible body of medical opinion.¹⁷ However, the Supreme Court of India has increasingly emphasized the Bolitho Test in the case of *Bolitho v City and Hackney HA*, which requires that the medical opinion also withstands logical analysis.¹⁸ In the context of AI, the Bolitho standard poses a high bar. A physician cannot simply argue that other doctors use this AI.¹⁹ They must demonstrate that using the AI was a rational choice in the specific case. This places an ethical and legal burden on clinicians to understand the rationale if not the exact technical mechanism of the tools they employ.²⁰ The traditional Bolitho inquiry asks whether a responsible body of practitioners would have acted similarly, a test premised on human professional judgement. Where an AI system generates a recommendation that no human practitioner would have independently reached, the standard is difficult to apply without modification. It may be necessary for courts to ask not to simply whether reliance on the AI was rational but whether the clinician exercised meaningful supervisory judgment over the AI's output such that they can genuinely be said to have made a clinical decision rather than merely endorsed an algorithmic one.

The Therac-25 Disaster case study is presented as a foundational illustration of the dangers of overconfidence in software reliability and the absence of adequate safety governance themes that are directly relevant to the accountability gaps disclosed in the preceding sections. It demonstrates how the concentration of design responsibility in a single developer combined with the removal of hardware failsafe, created conditions for catastrophic patient harm with no

¹⁶ *ibid.*

¹⁷ *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582 (QB).

¹⁸ *Bolitho v City and Hackney Health Authority* [1998] AC 232 (HL).

¹⁹ 'The Bolam Test: A Seismic Change in the Hon'ble Supreme Court's Stand on Its Acceptability' (2022) 44(3) *Journal of Indian Academy of Forensic Medicine* 2–6.

²⁰ Chloe Haden, 'The Consequences of the AI Act and Proposed AI Liability Directive on Medical Negligence: Will Physicians Fall Victim to "Red Tape" Rules?' (31 October 2024) 11 *Oslo Law Review* 1–9.

clear legal mechanism for redress. Between 1985 and 1987, the Therac-25 radiation machine delivered massive overdoses, killing or seriously injuring multiple patients. The software was written by a single programmer and reused code from older models that relied on hardware failsafe, because the Therac-25 removed these mechanical interlocks, a software race condition triggered high-energy beams.²¹ This remains the definitive cautionary tale of overconfidence in software reliability.²²

The Obermeyer case study provides a concrete illustration of how proxy-based algorithmic design can produce racially discriminatory clinical outcomes at scale and underscores the inadequacy of existing regulatory frameworks in preventing or remedying such harms. A landmark 2019 study published in *science* uncovered racial bias in a healthcare risk-prediction algorithm managing over 200 million people.²³ The developers used "historical healthcare spending" as a proxy for health needs. Because Black patients historically face barriers to access and spend less, the algorithm concluded they were healthier than equally sick White patients. This led to Black patients making up only 17.7% of those flagged for extra care, when their actual health conditions warranted 46.5%.²⁴

III. FRAGMENTED REGULATORY GOVERNANCE AND ACCOUNTABILITY GAPS IN HEALTHCARE AI

India lacks a specific law that regulates the use of artificial intelligence in the healthcare sector. Regulatory control is instead exercised through a fragmented collection of the general medical device regulation, professional rules, Consumer Protection Act, 2019 and Information Technology Act, 2000. Regulations of AI-based diagnostic and clinical decision-support systems of healthcare in India are mostly governed by the Medical Devices Rules 2017, which are framed by the Drugs and Cosmetics Act 1940 and are managed by the Central Drugs Standard Control Organisation (CDSCO). The MDR 2017 Rule 3(zb) provides the broader scope of software that is designed to be utilized in the diagnosis, prevention, monitoring, treatment or alleviation of disease, and as such, some AI tools can be considered Software as a Medical Device (SaMD).²⁵ Although the MDR framework presents pre-market approval,

²¹ Nancy G Leveson and Clark S Turner, 'An Investigation of the Therac-25 Accidents' (1987) IEEE Computer.

²² *ibid.*

²³ Miranda Khoury, 'Ensuring Equity in the Development of Health AI Algorithms' (BS thesis, University of Virginia, School of Engineering and Applied Science, Department of Biomedical Engineering, 2024).

²⁴ National Academies of Sciences, Engineering, and Medicine, Artificial Intelligence in Health Care: The Hope, the Hype, the Promise, the Peril (National Academies Press 2023).

²⁵ Medical Devices Rules 2017, r 3(zb), framed under the Drugs and Cosmetics Act 1940 (India).

conformity assessment, and risk-based classification under Rules 4 and 5, it is largely silent on how liability should be allocated for patient harm. Scholars have noted that the concept of MDR has the view of software as a fixed product, which does not consider the process of self-learning and adaptive algorithms that change after implementation.²⁶

The Digital Personal Data Protection Act, 2023 (DPDPA) is directly relevant to AI in healthcare as it regulates the processing of personal and health data. Section 4 stipulates that data should be processed with a lawful purpose, which in most cases is consent based, whereas in Section 6, the consent should be free, informed and specific, which is essential where AI systems are based on patient data.²⁷ Moreover, Section 8 imposes the responsibility on data fiduciaries, such as hospitals and AI creators, to secure data and stop data misuse. All these provisions are aimed at ensuring AI-powered healthcare systems are run in a framework of consent, accountability, and data protection.²⁸

The Consumer Protection Act 2019 is another legislation that covers AI-driven healthcare services. Section 2(42) incorporates medical services into the definition of service and Chapter VI (Sections 82-87) brings in a statutory product liability regime to manufacturers, service providers and sellers.²⁹ Theoretically, this allows patients to claim damages due to the fault of the malfunctioning AI systems or insufficient AI-based services.³⁰ In practice, though the evidentiary standards of Sections 84 and 85 assume that there exist some identifiable flaws, manufacturing mistakes, or a failure to warn, by which the culpability of AI developers can be proven.³¹ But this structure does not naturally apply to non-transparent, probabilistic AI systems, whose such apparent flaws may not be easily identified. Consequently, the point of care is likely to be the focus of liability rather than the design and development stage.

Information Technology Act, 2000 also makes allocation of liability difficult. Section 43A contains compensation liability regarding failure to safeguard sensitive personal data, whereas Section 79 provides safe-harbour to the intermediaries,³² who had the due diligence requirement under the Intermediary Guidelines of 2021.³³ According to scholars, this framework is not well suited to deal with AI systems that actively affect clinical outcomes as

²⁶ Timo Minssen and others, 'Regulating the Clinical Adoption of Artificial Intelligence' (2020) 28 Medical Law Review 1.

²⁷ Digital Personal Data Protection Act 2023, ss 4, 6.

²⁸ Digital Personal Data Protection Act 2023, s 8.

²⁹ Consumer Protection Act 2019, s 2(42).

³⁰ W Nicholson Price II, 'Medical AI and the Law' (2019) 23 Harvard Journal of Law & Technology.

³¹ Consumer Protection Act 2019, ss 84–85.

³² Information Technology Act 2000, ss 43A, 79.

³³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

opposed to being passive carriers of information. This means that developers and providers of platforms are often shielded against liability unless the harm can be defined as a data breach or cybersecurity breach.³⁴

The jurisdictions around the world have been more specific with the AI governance mechanisms, but accountability gaps still remain. In the Artificial Intelligence Act (2024) of the European Union, the majority of AI in the healthcare sector would be considered as the high-risk category and be subjected to conformity assessments, human supervision, reduction of bias elements, and post-market monitoring. Yet, researchers observe that the Act is not concerned with civil liability directly, shifting the compensation regulations to the preexisting tort and product liability frameworks and refraining from specifying liability on downstream harm.³⁵ In the United States, the regulation of AI in medical practice is built upon the SaMD framework by the Food and Drug Administration, which is concerned with safety and efficacy but does not specify liability in accordance with the harm in the future.³⁶

Combined, the Indian and global systems are primarily concerned with safety, ethics, and compliance rather than liability allocation. This is referred to by scholars as a layered and asymmetrical system of liability where the responsibility is formally distributed among regimes but substantially concentrated on clinicians and healthcare facilities.³⁷ This is indicative of a larger global trend of retrofitting AI governance into legal silos, leaving structural responsibility gaps in scenarios involving AI-induced medical injuries.³⁸

IV. POLICY ESSENTIALS FOR LIABILITY IN AI-DRIVEN HEALTHCARE

The current policy towards the regulation of artificial intelligence in healthcare in India needs to be re-oriented towards a consistent and accountable policy framework rather than merely adapting its statutes in bits and pieces. Lack of a specific healthcare AI regulatory framework has led to dependency on general regulatory tools that put more emphasis on safety and data

³⁴ Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* (Penguin Random House 2018).

³⁵ Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22 *Computer Law Review International* 97.

³⁶ US Food and Drug Administration, 'Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning-Based Software as a Medical Device' (FDA Discussion Paper, 2019).

³⁷ Benjamin H Lang and others, 'Responsibility Gaps in Artificial Intelligence Decision-Making' (2023) *Digital Society*.

³⁸ *Ibid*.

protection, but little on responsibility and liability³⁹. It is gradually becoming accepted by global policy consensus that AI in healthcare requires sector-specific regulation since it has direct implications on the right to health and patient safety, with a special reference to high-risk diagnostic and clinical decision-support systems.⁴⁰

It is also crucial that all the parties involved, clinicians, healthcare institutions, and AI developers, explicitly identify shared and tiered responsibility. Tiered responsibility implies distributing responsibility according to role and control: developers (first level) with design and algorithmic flaws, healthcare facilities (second level) with deployment and monitoring, clinicians (third level) with the ultimate decision. The allocation must be based on control, predictability of harm and avoidance of risk. This can be implemented by making changes in the Consumer Protection Act, 2019 and the Information Technology Act, 2000, as well as sector-specific regulations by CDSCO, which will provide clarity and legally binding responsibility.

Clinicians alone cannot be held responsible, as the distributed aspect of the AI-mediated decision-making process indicates that international policy organizations increasingly emphasize shared responsibility, whereas the developers of AI systems have control over the design, training data, and updates of the system.⁴¹ In practice, the AI developers often enter into contractual arrangements with hospitals and clinicians, allocating responsibilities between these actors clearly *ex ante* would be more appropriate in spreading the risk with its sources, and the courts would not need to conduct *ad hoc* attribution of liability⁴². Further, patients should be given the right to informed consent regarding the use of AI in their diagnosis and treatment. It should clearly include the nature, extent and any risks or limitations associated with it.

Moreover, the framework ought to recommend progressive fines or damages as a result of non-adherence or damages by AI systems. These can be monetary fines, deployment suspension, required corrective audits, and temporary usage prohibition. Regulators ought to be empowered to recall or retire AI systems where they find it to be unreliable or unsafe in instances of severe

³⁹ Ciro Mennella and others, 'Ethical and Regulatory Challenges of AI Technologies in Healthcare: A Narrative Review' (2024) 10 Heliyon.

⁴⁰ World Health Organization, Ethics and Governance of Artificial Intelligence for Health (WHO 2021).

⁴¹ OECD, Artificial Intelligence in the Health Sector: Policy Challenges and Opportunities (OECD Publishing 2022) 24–29.

⁴² European Commission High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI (2019).

or recurrent failures. These types of enforcement would help to make sure that everyone adheres, discourage carelessness, and promote trust in AI-based healthcare.

The regulatory framework used in India should be changed to be less of a one-time approval and more of a lifecycle-based model of AI systems. It should mandate continuous oversight through audit trails, strict version control, and compulsory re-validation after material algorithmic changes. The approvals have to be conditional, and periodic reviews and independent audit. In the absence of such mechanisms, approvals become ineffective and there are gaps in accountabilities; therefore, an explicit responsibility needs to be determined on developers, deployers, and end-users.

The changing and dynamic character of AI systems also require policy frameworks. Old approval paradigms are based on products that do not change and do not fit in the context of AI systems that evolve post-implementation. The regulators have pointed out the importance of lifecycle related oversight tools such as audit trails, version control and re-validation after material changes in the algorithm but in the absence thereof, regulatory approval may become null and thus third-party accountability may have lapses in the event of harm.

Lastly, institutional capacity is necessary in good governance. In practice, the international experience shows that specialised oversight bodies capable of converting the technical risks of AI into legal and regulatory standards that can be enforced would be beneficial in regulating consistency, improving judiciary decision-making, and increasing patient trust in India⁴³. Collectively, these policy interventions present a practical course of action towards balancing innovation and responsibility in AI-driven healthcare. India should instantiate this with a specialised institutional model either a dedicated AI Healthcare Regulatory Authority in the Ministry of Health or a specialised AI division within CDSCO, based on a Digital Health Centre of Excellence of the FDA. This organ is to be made up of interdisciplinary specialists and its role is to set standards, audit and guarantee lifecycle compliance. This kind of mechanism would facilitate consistency, accountability, and trust by mediating between the technical and legal enforceability.

V. CONCLUSION AND SUGGESTIONS

The integration of AI in the healthcare industry unveils a cardinal incompatibility between conventional negligence principles and the distributed nature of AI-based decision making. The current models overload clinicians even though developers and healthcare facilities play

⁴³ NITI Aayog, Responsible AI for All: A Policy Framework (Government of India 2021) 43–47.

an important role in determining clinical outcomes. The existing regulatory environment in India, including the Medical Devices Rules, Consumer Protection Act, Information Technology Act and the Digital Personal Data Protection Act, is still disjointed and is mostly concerned with safety and data protection, lacking a logical framework on how to apportion liabilities. A tiered responsibility framework is necessary to resolve this, with control and risk-based liability assigning the responsibility to developers, institutions, and clinicians, respectively. This should be backed by statutory intervention in order to prevent statutory dilution of developer liability.

In addition, regulation should also be changed to a lifecycle-based model, which needs to be constantly monitored by means of audit trails, version control, and re-validation of AI systems, with potentially effective sanctions such as suspension or retirement of unsafe systems. Informed consent to the use of AI should also be enhanced by means of patient autonomy. Lastly, a specialised regulatory body will have to be established as part of or in addition to CDSCO so that there are consistent oversight and translation of technical risks into enforceable standards. In the absence of these reforms, the current paradigms of law will remain accountability blind in AI-based healthcare. The future of AI in healthcare ultimately depends more on the legal system's ability to align responsibility with control, than on technological capability.

ORBITAL INJUNCTIONS: LEGAL REMEDIES FOR SATELLITE-BASED DIGITAL BLOCKADES

—Bhavya Rai*

ABSTRACT

The rapid proliferation of small satellite constellations and on-orbit serving technologies has given rise to a new and largely unregulated threat: the satellite communications blockade. Unlike terrestrial internet shutdowns or conventional cyberattacks, an orbital blockade operates from space itself, employing jamming, spoofing, or even physical interception of satellites to disrupt satellite communications and navigation services. This emerging form of coercion represents a novel mode of infrastructural aggression, exploiting structural gaps in international space law, telecommunications regulation, and existing remedies frameworks. In this context, this article introduces the notion of the “orbital blockade,” and gives illustrations that clearly indicate that interference in space can lead to immediate severe consequences for civilians, the economic system, or security infrastructures, which do not necessarily exceed the “threshold of armed conflict.” The main contribution of the article is the establishment of the new legal remedy called the Orbital Injunction. A jurisprudential basis for the Orbital Injunction is established by the synthesis of principles derived from the Outer Space Treaty, specifically Article IX’s obligations related to the prevention of harmful interference, the principles of the Radio Regulations adopted by the International Telecommunication Union, and the norm of “due regard” developing in customary international law. Secondly, this article will argue the case for a procedural approach that will allow quick assessments of evidence using space situational awareness information, accompanied by graduated enforcement. The article ends by emphasizing that in an increasingly congested, commercialized, and contested outer space the Orbital Injunction and other preventive legal measures are essential to prevent escalation and to uphold the principle that outer space must remain a peaceful province for the benefit of all humankind.

Keywords: *Space Law, Satellite Communications, Digital Blockade, Injunctive Relief, Outer Space Treaty, ITU Regulations, Cybersecurity, NewSpace, Infrastructure Warfare.*

* The author is a student at Rajiv Gandhi National University of Law, Punjab.

I. INTRODUCTION: THE NEW FRONTIER OF DIGITAL COERCION

On the 24th of February 2022, as the conventional warfare broke out in Ukraine, the less observable and equally deadly war raged in the EM spectrum and space. Reports started to come out about the jamming and cyber-attack on satellite internet communication systems, specifically the Viasat KA-SAT network.¹ Though the initial attack vector is ground-based cyber warfare, *this served as a critical warning regarding the impending danger of the direct use of space assets to implement the digital disruption.*² Indeed, the democratization of space access initiated by the emergence of space start-ups such as SpaceX (Starlink), OneWeb, and Planet Labs, combined with the militarization of space technologies, has now introduced a paradigm-changing risk of the satellite-based digital blockade.

The concept of a digital blockade based on satellites can be described as “the deliberate and targeted use of space-related assets and capabilities to frustrate, confuse, disrupt or destroy the satellite communication and data services of another state or non-state actor through a process that does not require traditional kinetic force.” The word targeted, by necessity, includes a notion of mens rea, differentiating an intentional blockade from any unintended consequences like the natural overlap of frequencies or bandwidth competition. Moreover, although it is a non-state actor who performs the blockade, according to the state responsibility principle in the Outer Space Treaty (Article VI), the internationally wrongful act of blockade will belong to the state responsible for the actions of the non-state actor. This is true both where the non-state actor has been authorized to perform the blockade and where the state is unable to stop the actions of the non-state actor.³

First, Electronic Warfare (“EW”) Inside Orbit: “Orbiting smaller satellites that carry jammers that saturate designated radio bands with noise, effectively interfering with satellites and land stations within a geographical area.” Second, Spoofing Satellites: This is carried out through transmitting deceptive and very powerful navigation (GPS/GNSS) signals from satellites above, leading to the failure and diversion of marine and air traffic and financial

¹ UK National Cyber Security Centre, ‘*Viasat Incident Report*’ (2022).

² US Space Command, ‘Space as a Warfighting Domain’ (2023) 2(1) *Journal of Space Security* 15, 19; EU Space Surveillance and Tracking (EUSST), ‘*Annual Report on Threats to Space Assets*’ (2024) 34.

³ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (opened for signature 27 January 1967, entered into force 10 October 1967) 610 UNTS 205, art 6; International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001) UN Doc A/56/83, art 8.

transactions.⁴ Third, physical blockading of satellites that is done through operating inspector satellites that can position themselves within line-of-sight between satellites and their terrestrial stations, effectively leading to a radio-frequency shadow zone.⁵

The thesis of this article is that a blockade of this kind signifies a peculiarly risky kind of infrastructural aggression, which occupies a legal twilight zone neither within the ambit of traditional war, cyberwarfare, nor peaceful exploitation of space. The current legal framework has a reaction-oriented mode that takes too long to respond effectively to a deed that can be completed in mere minutes, instigating a paralysis of society as well as the economy as a whole that does not amount to armed aggression under Article 51 of the Charter of the United Nations.⁶

An extensive literature search on the topic of space dispute resolution shows that although previous research has paid much attention to the limitations of the existing frameworks, such as the PCA Optional Rules for Arbitration of Disputes Relating to Outer Space Activities (2011), the International Court of Justice's ("ICJ") provisional measures according to Article 41 of its Statute, the ITU's non-binding measures on harmful interference per Article 56 of its Constitution, and new research on arbitration for harmful interference, no previous proposal has sought to address the lack of remedies equivalent to the Orbital Injunction.⁷ Previous literature has mostly been concerned with identifying the problem or discussing various forms of voluntary arbitration. None of the mechanisms discussed is time-efficient enough to resolve the conflict during a satellite blackout, none is based on SSAT data for a preliminary determination of whether to intervene, and no provisionally binding measures have been suggested to enforce such measures until the dispute settlement takes place. As far as I am aware, then, the Orbital Injunction represents a novel idea that fills a gap in the existing literature. In this critical void, this paper proposes the legal tool of the Orbital Injunction. The

⁴ Todd E Humphreys, 'Statement on GPS Spoofing' (US House Committee on Science, Space and Technology, 9 October 2012) 3–5; Dana A Goward, 'Maritime GPS Spoofing: A Growing Threat' (2023) 44(2) *Journal of Navigation* 112, 118.

⁵ Michael Listner, 'The Legal Implications of "Inspector" Satellites and Proximity Operations' (2021) 44(3) *Journal of Space Law* 213, 220–225; Moriba Jah, 'The Emerging Threat of Radio Frequency Shadow Zones in LEO' (2022) 12(1) *Astropolitics* 31, 38.

⁶ Charter of the United Nations art 51; UN General Assembly, *Definition of Aggression* (1974) UNGA Res 3314 (XXIX), art 3.

⁷ Permanent Court of Arbitration, *Optional Rules for Arbitration of Disputes Relating to Outer Space Activities* (2011); Statute of the International Court of Justice art 41; Constitution and Convention of the International Telecommunication Union (Geneva 1992) art 56; S Pratidina, F Latipulhayat and R Handayani, 'Arbitration as a Method of Settling Harmful Interference Disputes in Satellite Communications' (2024) 15(2) *Indonesian Journal of International Law* 201; S Aoki, 'Malicious Cyber Activities Against Space Assets: An ITU and Space Law Perspective' in M Hofmann (ed), *Cybersecurity in Outer Space* (Nomos 2024) 89–112.

Orbital Injunction shall be defined as a swift, binding provisional decision of an appropriate international adjudicatory authority requiring a state or entity to desist from space-based means of harmful interference. It shall represent the legal equivalent of the circuit breaker, which serves to defuse a situation to allow for a full resolution to be made.

The discussion will unfold over four sections. Part II will describe the technical reality of orbital blockades, demarcating their viability and uniqueness over cyber activities on Earth. Part III will undertake a critical diagnosis of the current legal instruments that can be applied to the scenario: space law, telecommunications law, and the law of state responsibility. The inadequacies of these instruments will come to light. Part IV will form the heart of the discussion. The conceptual framework of the Orbital Injunction will evolve within these sections. The legal foundation, procedural requirements, standards of evidence, and modalities of enforcement of the Orbital Injunction will be established. Part V will engage with real-world challenges. Conclusion will justify the need for the Orbital Injunction in governing space in the 21st century.

II. THE ANATOMY OF AN ORBITAL BLOCKADE: TECHNICAL FEASIBILITY AND TYPOLOGY

To ground the legal discussion, one must first understand the technical vectors of attack. The NewSpace revolution has made possible what was once the domain of superpowers.

A. The Enabling Technologies

There are four critical technologies that make orbiting blockades possible. First, SmallSats and CubeSats cost very little money to build and deploy and could possibly either have jamming capability on board or serve as obstruction devices.⁸ Second, technologies involving docking, handling, and manipulating of spacecrafts in outer space such as Northrop Grumman's Mission Extension Vehicle could be used for trailing, obstruction, or even capturing the enemy satellite.⁹ Third, using software-defined radios ("**SDRs**") could redirect the jamming capabilities of a satellite on various frequencies, thus masking the origin of the jamming attack.¹⁰ Finally, there

⁸ Fraunhofer EMI, 'Small Satellite ERNST: First Image Data from the Thermal Infrared Camera' (2025); US Missile Defense Agency, 'CubeSat Networked Communications Experiment (CNCE) Block 1' (2021).

⁹ Northrop Grumman, 'SpaceLogistics: In Orbit Satellite Servicing'; Northrop Grumman, 'Mission Extension Vehicle (MEV)' (2020).

¹⁰ Per Vices, 'Software Defined Radio Use Case for Satellite Industry' (*everything RF*, 23 March 2022); Jean Michel Friedt, Gwenhaël Goavec Merou and François Meyer, 'Software Defined Radio Implemented GPS Spoofing and Its Computationally Efficient Detection and Suppression' (2021) *HAL Archives*.

is a newer type of satellite referred to as an inspector satellite which has performed uncomfortably close manoeuvres around other nations' space-based equipment.¹¹

B. Three Scenario-Based Typologies

1.) Scenario 1: The Selective Jamming Constellation (The "Digital Siege")

State A has a territorial dispute with State B and develops an orbit of six mini-satellites in Low Earth Orbit. On command, they begin to emit jammers with powerful cones of interference against State B's territorial areas and military zones. The result is that no broadband, GPS, or cellular backhaul connectivity is possible in these areas, and this is achieved without even firing a single bullet in the affected region.

2.) Scenario 2: The Spoofing Satellite (The "Phantom Menace")

The satellite owned by the state, disguised as a communications satellite, is maneuvered into a strategically critical position near an important geographical choke point such as the Strait of Hormuz. It commences broadcasts of false GPS information. Ships using the GPS system begin receiving faulty directions for their route, leading to dangerous situations such as near collisions, ship grounding, or being led into hostile waters. The results can be catastrophic and immediate. This scenario is not a theoretical possibility; in August 2019, the US Maritime Administration (**"MARAD"**) warned vessels in operation within the Persian Gulf, Strait of Hormuz, and Gulf of Oman that they may be facing GPS interference, bridge-to-bridge communications spoofing, and/or other communications jamming with little to no warning.¹² At least two ships reported experiencing GPS interference, and US defence officials have confirmed that the Iranian authorities have installed GPS jammers on Abu Musa Island, located at the entrance of the Strait of Hormuz, with the objective of interfering with navigational systems and thereby seize vessels.¹³ The convergence of GPS spoofing, seizing of ships, and geography of the global choke point has thus been empirically established in support of the orbital blockade hypothesis put forward in this article.

3.) Scenario 3: The Kinetic Blocker (The "Orbital Bully")

The term inspector satellite describes a satellite owned by State X, which uses its propulsion to position itself repeatedly between a critical reconnaissance satellite owned by State Y and

¹¹ US Department of Defense, 'Space Situational Awareness and Inspector Satellites' (2023); Brian Weeden and Victoria Samson (eds), *Global Countdown: Space Security Index 2024* (Secure World Foundation 2024) 45–48.

¹² US Maritime Administration (MARAD), *MSCI Advisory 2019-012* (7 August 2019).

¹³ Barbara Starr and Ryan Browne, 'US Government Warns of Iranian Threats to Commercial Shipping, Including GPS Interference' CNN (7 August 2019); 'Cyber Interference against Vessels in the Persian Gulf and Gulf of Oman (2019)' (CCDCOE Cyber Law, 2021).

its primary ground station, creating a radio frequency shadow, eliminating State Y's ability to download critical image information during an emergency situation. State X disguises its actions as proximity operations.

These are not science fiction scenarios but the projection of known capabilities. The linking factor for all these scenarios is the use of orbital positioning for terrestrial force, in the grey area that is short of war.

In all three hypothetical situations provided above, it is a state actor who acts as a perpetrator of an alleged violation of international law. According to Article VI of the Outer Space Treaty and the Articles on State Responsibility, non-state activities will lead to international disputes if they can be attributed to a certain state, for example, due to a lack of control over a private entity by that state. A purely private blockade falls under the jurisdiction of national law.¹⁴

III. THE LEGAL LACUNA: WHY CURRENT FRAMEWORKS FAIL

No single legal regime was designed to address the specific challenge of a rapid-onset, state-orchestrated digital blockade from space.

A. International Space Law: Broad Principles, Weak Remedies

The Outer Space Treaty, 1967, remains a weak and enabling tool for the governance of outer space.¹⁵ Outer Space Treaty provisions are inadequate for tackling orbital blockades.¹⁶ Article I of the treaty stipulates the use of outer space in accordance with international law, for peaceful purposes which is obviously breached whenever access is denied to a particular country. Article III of the treaty contains the ban on threat or use of force which is a provision from the UN Charter Article 2(4), but the legal status of the act of electronic blockade remains politically controversial and hard to prove.¹⁷ Article VI of the treaty makes states liable for activities conducted by entities under their jurisdiction, but offers no recourse for addressing such problems.¹⁸ More importantly, Article IX of the treaty obliges states to refrain from interfering with the activities of other states and engage in consultations if so requested.¹⁹

¹⁴ International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001) UN Doc A/56/83, art 8; International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (2001) UN Doc A/56/10, 103–107.

¹⁵ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (opened for signature 27 January 1967, entered into force 10 October 1967) 610 UNTS 205.

¹⁶ *ibid*, art 1.

¹⁷ Charter of the United Nations art 2(4).

¹⁸ *ibid*, art 6.

¹⁹ *Ibid*, art 9.

B. International Telecommunication Union (ITU) Regulations: Technical, Not Political

The ITU's Constitution, Convention, and Radio Regulations collectively mandate that radio frequency spectra and orbital resources be used in a manner that avoids harmful interference.²⁰

1.) No. 15.1 of the Radio Regulations: No harmful interference may be caused. Interference which could endanger the functioning of a radionavigation service or of other safety services or seriously degrade, obstruct, or repeatedly interrupt a radiocommunication service is considered harmful interference.²¹

2.) ITU's Role: It is a technical coordinating body. Its method of settling a dispute (Article 56 of the Constitution) is slow, diplomatic, and looks for a compromise. While an ITU determination of harmful interference has great moral authority, it is non-binding. A State conducting a deliberate blockade has already manifested itself to be of bad faith and will not be bothered by an ITU advice.²²

C. The Law of State Responsibility & The UN Charter: Too High a Threshold

Under the International Law Commission's Articles on State Responsibility ("ARSIWA"), an intentional satellite or electronic blockade constitutes an internationally wrongful act, breaching both the Outer Space Treaty and the ITU regime. Such a breach triggers the duties of cessation and non-repetition under Article 30, as well as full reparation under Article 31; yet again, the actual implementation of ARSIWA is dependent on diplomatic efforts or judicial settlement and is thus not functionally capable of dealing effectively and quickly in a fast-breaking crisis situation.²³ In a similar manner, although Chapter 7 of the UN Charter formally authorizes the Security Council to take measures to implement a determination made under Article 39 of the existence of a threat to the peace, breach of the peace, or act of aggression, a digital or electronic blockade is not likely to fall within that description and could not effectively be implemented anyway due to the probable exercise of a Security Council veto if the act is traceable to or supports a permanent Security Council member.²⁴

²⁰ Constitution and Convention of the International Telecommunication Union (adopted 22 December 1992, entered into force 1 July 1994) 1825 UNTS 1; International Telecommunication Union, *Radio Regulations* (2020 ed).

²¹ International Telecommunication Union, *Radio Regulations* (2020 ed) No 15.1.

²² *ibid*, art 56.

²³ International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001) UN Doc A/56/83.

²⁴ Charter of the United Nations arts 39, 41, 42.

D. International Humanitarian Law (IHL): Only Activated in Armed Conflict

In an international armed conflict, the IHL principles of distinction and proportionality may apply to a blockade. Nevertheless, it is just because of blockades in situations of peace/grey zone conflict that strategic advantages are gained without resorting to a war in situations where a war is unwanted. IHL is a post facto legal tool, not a preventive one. The cumulative weakness of these regimes is one of speed and specificity. The regimes provide for condemnation following the violation or arbitration on a slow track, but do not provide for relief on an urgent and specific basis to stop the violation in progress. Such a weakness gives leeway to orbital force.²⁵

IV. CONSTRUCTING THE ORBITAL INJUNCTION: DOCTRINE AND PROCEDURE

All the problems mentioned in Part III, lack of a cessation requirement alongside Article IX's obligation to engage in consultation, the ITU's non-binding and lengthy process, the stringent conditions of invoking the UN Charter's prohibition of the use of force, and the limited application of IHL in situations outside of armed conflict, suffer from a similar problem of lacking a rapid and binding provisional solution. The Orbital Injunction remedies this deficiency. First, its doctrine rests upon the rule against harmful interference established by Article IX, the precedent of provisional measures before international tribunals, and the customary norm of due regard. Second, its process is intended to be fast and scientifically credible through the use of SSA information and the prima facie case and likelihood of irreparable injury criteria. Third, its enforcement hierarchy provides a legitimate option between no action and kinetic reaction.

The Orbital Injunction is proffered as a sui generis remedy specific to and for the specific domain that is outer space and for digital blockades. It is supported and reinforced through analogies that are drawn from interlocutory injunctions and provisional measures that are applicable under public international law

²⁵ Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287, art 33; Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, arts 48, 51, 52, 57.

A. Legal Foundations and Analogous Principles

1) Article IX OST as the Substantive Hook: The duty not to cause potentially harmful interference and the duty to consult comprise the rule of law alleged to be breached.²⁶ The injunction preserves rights pending the consultations, or subsequent adjudication, whichever may be the outcome.

2) Interim Measures in International Adjudication: Under international law, the International Court of Justice and the International Tribunal for the Law of the Sea are authorized to indicate provisional measures to preserve the respective rights of parties under dispute. ICJ Statute, Article 41; UNCLOS, Article 290. The Orbital Injunction is thought of as a special kind of provisional measure for space-related disputes.²⁷

3) The Due Regard Principle: This principle is long established in the law of the sea and air law, is increasingly recognized as an operative norm in space law. Its status is supported by the 2019 COPUOS Long-term Sustainability Guidelines (Guideline 2.2), the MILAMOS Project's treatment of due regard as a foundational rule for peacetime military activities, and the 2013 UN GGE report on TCBMs subsequently endorsed by UNGA resolutions. A satellite-based digital blockade constitutes an exemplary failure of due regard, justifying urgent intervention.²⁸

B. Forum and Procedure: Where and How to Seek an Orbital Injunction

A critical challenge is identifying the competent forum. Three potential pathways exist, with a proposed new hybrid model being optimal.

1) Pathway A: ICJ Provisional Measures

A state may seek to seize the International Court of Justice by framing the dispute as one concerning the interpretation or application of the Outer Space Treaty and request the indication of provisional measures; however, this avenue is fraught with structural limitations, as ICJ jurisdiction is contingent upon state consent, proceedings are inherently protracted, and the Court has historically exercised considerable restraint in granting urgent relief, particularly in

²⁶ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (opened for signature 27 January 1967, entered into force 10 October 1967) 610 UNTS 205, art 9.

²⁷ Statute of the International Court of Justice (adopted 26 June 1945, entered into force 24 October 1945) 15 UNCTAD 355, art 41; United Nations Convention on the Law of the Sea (opened for signature 10 December 1982, entered into force 16 November 1994) 1833 UNTS 3, art 290.

²⁸ UN Committee on the Peaceful Uses of Outer Space, *Guidelines for the Long-term Sustainability of Outer Space Activities* (2019) UN Doc A/74/20, Annex II, Guideline 2.2; McGill Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS) (2022) vol I, rule on 'Cooperation, Mutual Assistance and Due Regard'.

technically complex and highly specialized domains, thereby rendering it an ineffective mechanism for timely redress in fast-evolving space-related crises.

2) Pathway B: ITU Administered

A new protocol to the ITU Convention could create a permanent panel of technical and legal specialists with the authority to conduct emergency arbitration in situations of harmful interference in satellite communications, and the key advantage of this approach is the ITU's unmatched technical know-how and experience in managing spectrum and resolving interference disputes. However, the key disadvantage is of a more structural and political nature, the need for a formal change to the existing treaty and a strong will on the part of states to cede national discretion and political capital to the requirement of compulsory and technical decision-making.

3) Pathway C (Proposed): “Space Situational Awareness (SSA) Consortium Tribunal.”

This is the most innovative and promising approach. Already existing providers of SSA (such as the Space Surveillance Network, LeoLabs, or commercial entities) are monitoring objects and capable of defining anomalies (for example, when a satellite begins to emit jamming patterns or when it behaves aggressively).²⁹ A group of providers, together with an existing arbitration institution. For example, the Permanent Court of Arbitration (“PCA”), could work out an emergency pre-existing pattern to solve any dispute. The affected state will submit its SSA information as evidence to an emergency arbitrator or panel of arbitrators at PCA in case of an emergency. They have the authority to issue an Orbital Injunction in no time.³⁰

C. The Injunction Standard: A Two-Pronged Test

In order to secure an Orbital Injunction, the petitioner state must meet a heavy but possible burden of proof:

1) Prima Facie Case of Harmful Interference: Evidence, based on credible expert proof (SSA data, signal analysis from ground stations), must show a high probability that the respondent's space object is causing deliberate harmful interference to the peaceful use of space by the petitioner.

²⁹ US Space Command, ‘Space Surveillance Network’ (2023); LeoLabs, ‘Low Earth Orbit Tracking and Monitoring’ (2024).

³⁰ Permanent Court of Arbitration, *Optional Rules for Arbitration of Disputes Relating to Outer Space Activities* (2011).

2) Risk of Irreparable Harm & Urgency: Continued activity causes or threatens to bring about irreparable harm to: (i) National security; (ii) Public security (e.g., air marine transport); (iii) Humanitarian needs; (iv) The space environment (risk of collision as a consequence of spoofing). Here, the element of urgency will automatically be satisfied.

D. Enforcement: From Legal Order to Physical Compliance

The “Achilles’ Heel” of any international injunction is enforcement. A layered approach is necessary:

1) *Phase 1: Naming and Shaming & Diplomatic Isolation*: The publishing of the injunction in the forum, coupled with the technical evidence, triggers international diplomatic action against the offender.

2) *Phase 2: Collective Responses*: Other nations and private operators would be invited to undertake proportionate countermeasures. These could include a cyber counter-jamming response to disable the jamming module of the delinquent satellite as a lawful countermeasure under ARSIWA Article 22³¹ an orbital shunning response, whereby the worldwide community of commercial satellites would move away from any relationship with the offender’s satellites, effectively isolating them and the activation of existing financial sanctions against those involved.

3) *Phase 3: Defensive Physical Actions (Last Resort)*: In a final resort option only after being specifically sanctioned by the UN Security Council or as a principle of collective self- defence in situations where the blockade has escalated to the point of an armed attack, countries can use a least destructive force, in which case a specific example of a directed-energy weapon might be used to destroy the malicious satellite’s payload. This is fraught with risks of escalation and debris creation and must be subject to the strictest IHL principles.

E. Cyber Counter-Jamming as a Lawful Countermeasure

According to Article 22 of the ARSIWA, one state is allowed to employ countermeasures in response to another’s internationally wrongful act, as long as the measure is meant to bring about compliance while satisfying stringent criteria. Regarding a cyber-attack that disables only the jamming module of a renegade satellite by injecting code that causes a software reboot or interrupts the command link, there are five criteria that should be satisfied for the conduct to amount to a lawful countermeasure. First, the interference of the blocking state should itself be an internationally wrongful act and violation of Article IX of the OST and ITU Radio

³¹ International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001) UN Doc A/56/83, art 22.

Regulations.³² Second, the cyber activity should be proportional to the harm inflicted on the former as per ARSIWA Article 51³³ damaging the jamming capability of the satellite is generally a proportionate action, while damaging the entire satellite is not. Third, the measure should not involve the use of prohibited force according to Article 2(4) of the UN Charter; non-destructive cyber actions are allowed, while physical destruction is permitted only in Phase 3.³⁴ Finally, procedural obligations, a previous request for cessation and notice, exist, although urgent situations might necessitate immediate measures to avoid irreparable damage as per ARSIWA Article 52(2). If all these criteria are met, cyber counter-jamming can be considered a legal and non-violent way to stop an existing space blockade.

V. CHALLENGES AND THE IMPERATIVE FOR PRE-EMPTIVE LEGAL ARCHITECTURE

No legal remedy is immune from practical difficulties. The Orbital Injunction faces three persistent challenges: attribution of hostile acts to a specific state; dual-use ambiguity that masks aggression as legitimate activity; and the risk of escalation. Addressing these candidly is essential to strengthen, not dismiss, the proposal. This is prone to risks of escalation and generation of debris and has to be governed by the most stringent IHL principles. Confronting Practical Challenges are given below:

A. Attribution

Attribution is less acute in space than in cyberspace. Space situational awareness (“SSA”) networks continuously track satellite positions, manoeuvres, and radio frequency emissions.³⁵ The Registration Convention requires states to declare each satellite’s function; deviation from that function e.g., a registered telecom satellite engaging in jamming supports a prima facie case.³⁶ The evidentiary standard for an injunction is high probability, not criminal proof, which SSA data and ground-based signal monitoring readily satisfy.

B. Dual-Use and Ambiguity

³² *ibid* art 9; International Telecommunication Union, *Radio Regulations* (2020 ed) No 15.1.

³³ *ibid* art 51.

³⁴ Charter of the United Nations art 2(4); *ibid* art 50(1)(a).

³⁵ US Space Command, ‘Space Surveillance Network’ (2023); LeoLabs, ‘Low Earth Orbit Tracking and Monitoring’ (2024); European Union Space Surveillance and Tracking (EUSST), *Frontier 2.0: Space Surveillance and Tracking Support Framework* (2025).

³⁶ Convention on Registration of Objects Launched into Outer Space (opened for signature 14 January 1975, entered into force 15 September 1976) 1023 UNTS 15, arts 2, 4.

A violating state may claim its satellite is conducting scientific research or testing. The Orbital Injunction employs an effect- based standard under Article IX of the Outer Space Treaty and ITU Radio Regulations:³⁷ harmful interference is defined by objective impact on safety services and communications, not by intent. Independent technical assessment via SSA and ITU monitoring distinguishes deliberate jamming from benign activity. A state genuinely engaged in research can easily demonstrate compliance; persistent interference reveals bad faith.

C. Risk of Escalation

An injunction could escalate a grey-zone conflict. However, the Orbital Injunction is designed as a de-escalatory tool: it provides an off-ramp through compliance with a neutral ruling, internationalises the dispute, and employs a graduated enforcement ladder, beginning with diplomatic pressure, moving to collective countermeasures, and reserving defensive physical action only as a last resort, subject to UN Security Council approval or Article 51 self-defence.³⁸ Safeguards include multi-member panels, exhaustion of consultations, and strict IHL compliance for any kinetic response.³⁹

D. The Imperative for Pre-emptive Legal Architecture

Attribution, dual-use ambiguity, and escalation risk are manageable with existing SSA technology, effects-based standards, and layered procedures. The current legal vacuum is more dangerous than these challenges. Pre-emptive adoption of the Orbital Injunction framework would deter aggression, reassure states, and preserve outer space as a peaceful global common.

VI. CONCLUSION: PRESERVING THE ORBITAL COMMONS FOR THE FUTURE

Outer space is a vital global common and the foundation of the modern digital economy. Satellite-based digital blockades pose an immediate and serious threat to international peace, security, and economic stability. Yet existing legal frameworks offer only delayed justice which, against an instantaneous and crippling attack, amounts to justice denied. The Orbital Injunction is not a panacea, but it constitutes a necessary and feasible step toward a more

³⁷ *ibid*, art 9; International Telecommunication Union, *Radio Regulations* (2020 ed) No 15.1.

³⁸ Charter of the United Nations art 51.

³⁹ Constitution and Convention of the International Telecommunication Union art 56; International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001) UN Doc A/56/83, arts 30, 31; Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, arts 48, 51, 52, 57.

resilient legal order for space. Building on existing SSA infrastructure and adapting time-tested concepts of provisional relief, the international community can construct a swift, credible, and proportionate response to infrastructural aggression in space.

A. The SSA Consortium Tribunal:

The most original and valuable pathway proposed in this article is Pathway C, the SSA Consortium Tribunal. To move from conceptual sketch to actionable recommendation, the following specifications are essential. First, the standing panel of arbitrators should comprise fifteen members: five space law experts nominated by the Permanent Court of Arbitration (PCA), five technical experts (e.g., satellite engineers, radio frequency specialists) nominated by the ITU and five experts in space situational analysis nominated by a consortium of SSA data providers, e.g., LeoLabs, the US Space Surveillance Network, and the European Union Space Surveillance and Tracking (EUSST) partnership. Second, authentication of SSA data would be achieved through a cryptographic chain-of-custody protocol: raw tracking data such as ephemeris, time stamps, radio frequency fingerprints would be hashed and signed by at least two independent SSA providers before submission, with the panel empowered to appoint a neutral technical expert to verify authenticity in contested cases. Third, the trigger threshold for emergency situation is met when (a) a petitioner state presents SSA data showing a high probability of ongoing harmful interference as defined by ITU Radio Regulations No. 15.1, and (b) the interference directly endangers safety services, aviation, maritime, emergency communications or causes irreparable economic or security harm. No prior exhaustion of diplomatic consultations is required in such emergency circumstances. Fourth, service of the injunction on a respondent state would be affected by simultaneous submission to the state's UN mission, its national space agency, and, where practicable, direct transmission to the command link of the offending satellite via internationally coordinated notification frequencies, e.g., the ITU's International Monitoring System. The injunction becomes binding upon transmission; non-compliance triggers the graduated enforcement ladder set out in Section IV.D.

B. Amendment to Article IX of the Outer Space Treaty:

The substantive hook for the Orbital Injunction is Article IX, which currently obligates states to consult upon request but imposes no duty to cease potentially harmful conduct pending consultation. To give this obligation procedural teeth, this article recommends the adoption of an Optional protocol to the Outer Space Treaty Concerning Urgent Interim Measures for Harmful Interference. The Protocol would add a new paragraph to Article IX, reading as:

If a State Party has reasonable grounds to believe that a space object launched by another State Party is causing harmful interference to its peaceful exploration and use of outer space, and if such interference poses an imminent threat to safety services or critical infrastructure, the requesting State may submit an application for an emergency interim measure to a panel of arbitrators constituted under the auspices of the Permanent Court of Arbitration. The panel shall issue a binding interim order requiring the cessation of the alleged interference within 72 hours of application, provided the requesting State establishes a *prima facie* case and a risk of irreparable harm. The order shall remain in force pending final resolution of the dispute or until the panel determines that the interference has ceased. The duty to consult under the preceding sentence shall not excuse compliance with an interim order.

This Protocol transforms the soft-law duty to consult into a hard-law duty to submit to emergency adjudication and to comply with binding provisional relief. It would be optional, allowing states to opt into the mechanism without amending the OST itself, thereby lowering the political barrier to adoption.

The alternative to such legal innovation is a zone of chaos and might-makes-right politics, where states prove their determination through destabilizing space manoeuvres, leading to potentially disastrous conflict through misjudgement. The decision to regulate a new frontier through law rather than brute force has never been more pressing. The development of the Orbital Injunction doctrine, including the specific proposals for an SSA Consortium Tribunal and an Optional Protocol to Article IX, should begin now, not after the first catastrophic blockade.