THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES, KOCHI

DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF MASTER OF LAWS IN INTERNATIONAL TRADE LAW (2024 - 2025)

ON THE TOPIC

Artificial Intelligence and Digital Global Trade: Addressing Regulatory Challenges

Under the Guidance and Supervision Of

Dr. ANIL R. NAIR, ASSOCIATE PROFESSOR

THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES, KOCHI

Submitted by: **T J ALOK**

Register No: **LM0224021**

LL.M. (INTERNATIONAL TRADE LAW)

CERTIFICATE

This is to certify that **T J Alok**, REG NO: **LM0224021** has submitted his Dissertation titled – "**Artificial Intelligence and Digital Global Trade: Addressing Regulatory Challenges**" in partial fulfilment of the requirement for the award of Degree in Master of Laws in **International Trade Law** to the **National University of Advanced Legal Studies, Kochi** under my guidance and supervision. It is also affirmed that the dissertation submitted by his is original, bona fide and genuine.

Date: **28th May, 2025**
Place: **Ernakulam**

Dr. Anil R. Nair, Associate Professor
GUIDE AND SUPERVISOR
NUALS, KOCHI

DECLARATION

I, **T J Alok**, do hereby declare that this dissertation work titled "**Artificial Intelligence and Digital Global Trade: Addressing Regulatory Challenges**" researched and submitted by me to **the National University of Advanced Legal Studies** in partial fulfilment of the requirement for the award of degree of Master of Laws in **International Trade Law** under the guidance and supervision of **Dr. Anil R. Nair**, **Associate Professor**, **the National University of Advanced Legal Studies** is an Original, Bonafide and Legitimate work. It has been pursued for an academic interest. This work or any type thereof has not been submitted by me or anyone else for the award of another degree of either this university or any other university.

Date: **28th May, 2025**
Place: **Ernakulam**

T J ALOK
Reg.NumberLM0224021
LL.M., International Trade Law
NUALS, Kochi

ACKNOWLEDGEMENT

I have taken sincere efforts and hard work to complete this Dissertation within the prescribed time frame. However, it would not have been possible without the kind support and guidance from certain people who require a special acknowledgement. My Dissertation, "*Artificial Intelligence and Digital Global Trade: Addressing Regulatory Challenges"* would not have been completed if I do not acknowledge those who helped me to complete it within time.

At the outset, I would like to take this opportunity to express my profound respect and deep sense of gratitude to **Dr. Anil R. Nair, Associate Professor, Chairperson, Centre for Post Graduate Legal Studies and Director, Centre for Parliamentary Studies and Law Reforms** for his support, guidance and encouragement throughout the course of research work.

I would also like to extend my gratitude to the Vice Chancellor, **Hon'ble Mr. Justice S. Siri Jagan (Retd.)** for his constant encouragement and support. I would also like to extend my heartfelt gratitude to all the faculties of NUALS for their constant encouragement and support throughout the course of research work.

I am thankful and blessed to have my friends **Mr. Bharath Sankar, Mr. Akhil Remesh Nair and Ms. Samyukta P Menon** who too have travelled their journey with their dissertation with me and if not for their push, it would not have been possible for me to complete this dissertation.

All of this would not have been possible if not for the absolute love, encouragement and support of my family, sister, especially I owe my deepest gratitude to my beloved mother, **T Vinitha Jagannath,** whose unwavering love, silent sacrifices, and constant prayers have been the bedrock of my journey. Her strength and unconditional support have inspired me every step of the way and this work stands as much a reflection of her devotion as it is of my effort and I shall forever be grateful for their constant presence of positivity during the course of this Dissertation.

I begin by offering my humble pranāms to the Almighty—**Parmathma**—whose divine grace (kripā) and guidance have sustained me through this academic journey. May His blessings continue to illuminate my path with wisdom (jñāna) and perseverance (shraddhā).

T J ALOK

LIST OF ACRONYMS AND ABBREVIATIONS

&	And
AI	Artificial Intelligence
AML	Anti-Money Laundering
BPO	Business Process Outsourcing
CAC	Cyberspace Administration of China
CCPA	California Consumer Privacy Act
CTF	Counter-Terrorism Financing
DPDP Act	Digital Personal Data Protection Act (India)
EU	European Union
FATF	Financial Action Task Force
FTA	Free Trade Agreement
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDPR	General Data Protection Regulation (EU)
ICT	Information and Communication Technology
IMO	International Maritime Organization

IPEF	Indo-Pacific Economic Framework
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
IT Act	Information Technology Act (India)
ITU	International Telecommunication Union
JSI	Joint Statement Initiative
LDCs	Least Developed Countries
LGPD	Lei Geral de Proteção de Dados (Brazilian Data Protection Law)
MASS	Maritime Autonomous Surface Ships
MeitY	Ministry of Electronics and Information Technology (India)
MFN	Most-Favoured-Nation
NAGA	National AI Governance Authority (Proposed)
NDAP	National Data and Analytics Platform (India)
NIST	National Institute of Standards and Technology (U.S.)
NITI Aayog	National Institution for Transforming India (Policy Think Tank)
OECD	Organisation for Economic Co-operation and Development
RBI	Reserve Bank of India

RCEP	Regional Comprehensive Economic Partnership
SaaS	Software-as-a-Service
SC	Supreme Court (India)
SEBI	Securities and Exchange Board of India
SMEs	Small and Medium Enterprises
TRAI	Telecom Regulatory Authority of India
UNCTAD	United Nations Conference on Trade and Development
UPI	Unified Payments Interface (India)
WCO	World Customs Organization
WTO	World Trade Organization

S. No.	**Statute / Legal Instrument**	**Jurisdiction / Type**
1	Information Technology Act, 2000	India – National Legislation
2	Digital Personal Data Protection Act, 2023	India – National Legislation
3	Consumer Protection (E-Commerce) Rules, 2020	India – Regulatory Rules
4	General Data Protection Regulation (GDPR), 2016	European Union – Regulation

5	EU Artificial Intelligence Act (Draft, 2021)	European Union – Proposed Regulation
6	WTO General Agreement on Tariffs and Trade (GATT)	International – WTO Agreement
7	WTO General Agreement on Trade in Services (GATS)	International – WTO Agreement
8	WTO Agreement on Trade Facilitation	International – WTO Agreement
9	UNCTAD Digital Economy Reports	International – UNCTAD Framework
10	OECD Principles on Artificial Intelligence, 2019	International – Soft Law Principles
11	NIST AI Risk Management Framework	United States – Non-Binding Framework
12	FATF Recommendations on Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF)	International – Financial Regulation
13	Chinese Algorithm Regulation Guidelines (CAC, 2022)	China – National Regulation
14	ISO/IEC 23894:2023 – AI Risk Management Standard	International – Technical Standard (ISO)
15	ISO/IEC TR 24028:2020 – Trustworthiness in AI	International – Technical Standard (ISO)
16	Recommendation ITU-T Y.3172 – Framework for AI Trustworthiness	International – ITU Recommendation
17	UNESCO Recommendation on the Ethics of Artificial Intelligence, 2021	International – UN Soft Law

LIST OF CASES

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
- Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
- General Agreement on Tariffs and Trade, Oct. 30, 1947, 55 U.N.T.S. 194.
- General Agreement on Trade in Services, Apr. 15, 1994, 1869 U.N.T.S. 183.
- U.S. Dep't of the Treasury, OFAC Enforcement Action Against Amazon (2020).
- Alibaba Export Compliance Investigation (2021)

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Artificial Intelligence (AI) technologies have percolated virtually in every aspect of global trade, transforming traditional business practices and revolutionizing the way commerce is conducted. AI, broadly defined as the simulation of human intelligence processes by machines, encompasses a diverse array of technologies that enable computers to perform tasks that traditionally required human intelligence.

Global trade, according to world economic forum, is in constant flux, reshaped by technological breakthroughs that open new frontiers for commerce but also present fresh challenges for international trade policy. This was the case with the advent of the internet and the propagation of e-commerce, and it will be so with artificial intelligence. Given the sometimes-glacial pace at which multilateral policy-making moves, and the generalized and profound impact that AI will have on trade, there is an urgent need to build a policy architecture that reconciles trade and AI.[1]

With the rampant advancement and widespread usage of AI technologies, the integration of AI into global trade agreements poses significant challenges to existing legal frameworks as they were often drafted without much anticipation in this specific domain. Therefore, there is a pressing demand to address these legal complexities, thereby ensuring that international trade remains transparent, non-discriminatory, fair and conductive for economic bloom. By identifying gaps, analyzing existing legal frameworks, and proposing potential solutions, this research seeks to provide valuable insights into the development of AI inclusive trade policies and regulations.

In summary, this study seeks to illuminate the complex interplay between AI and global trade, emphasizing the critical imperative of addressing regulatory challenges.

---

[1] World Econ. F., *AI and Global Trade Policymaking*, World Econ. F. (Oct. 2024), https://www.weforum.org/stories/2024/10/ai-global-trade-policymaking/. (Last visited on Dec 26, 2024)

1.2 STATEMENT OF PROBLEM

The research paper aims to analyze the key regulatory challenges posed in digital trade, AI and their impact on the global economy and trade law.

1.3 RESEARCH PROBLEM

The integration of Artificial Intelligence (AI) into digital global trade possesses significant challenges, including cyber security risks, algorithmic bias market monopolization and ethical concerns. Without harmonized international framework and proactive international framework and proactive governance, these challenges may lead to systematic inequalities, reduces market competition and compromised trust in global systems.

1.4 RESEARCH QUESTIONS

- What are regulatory challenges in digital economy?
- What is global trade law and digital regulation?
- How to move towards harmonized digital trade regulations?
- How do international bodies like the OECD, EU, UNCTAD, GDPR, contribute to addressing AI and Digital trade Regulatory Challenges?
- How does the concept of digital trade sovereignty conflict with the principles of free trade?

1.5 RESEARCH OBJECTIVES

The main objectives of this research are;

- To Examine the regulatory challenges faced by countries on Artificial Intelligence and global trade
- To provide suggestions and propose modification for the universalization of the international trade framework, aimed at fostering trust, equity, and

- a healthy market competition within the global trade system.

1.6 RESEARCH METHODOLOGY

The study is purely doctrinal or non-empirical. The data collected is both primary and secondary. International agreements and treaties, national laws and policies, case laws and precedents and government and regulatory frameworks would be primary sources to understand the concept of Digital economy, Artificial Intelligence and Global trade in digital space, while Scholarly Articles, Legal Commentaries, Reports and policy Papers, UN and WTO Documents and AI-Specific Ethical Guidelines will be used as secondary sources. The collected data is summarized and interpreted in accordance with the research problem's requirements.

1.7 SCHEME OF THE RESEARCH

The following is the chapter structure of the research paper:

1. Introduction
2. Regulatory landscape of AI in Global Trade
3. Contribution of International bodies like OECD, GDPR, ISO, ITU etc.
4. India's legal framework governing AI and Digital Trade
5. Conclusion

In the present work, the following scheme of research has been used:

1. The second chapter, titled 'Regulatory landscape of AI in Global Trade,' delves into the regulatory challenges, particularly in liability for AI-related trade errors, biases in automated decision-making and fragmented global standards on AI usage. These issues complicate trade regulations as current framework lacks specific guidelines for AI, necessitating global cooperation to develop standards that ensures transparency, accountability and fairness in trade agreements.
2. The third chapter, titled 'Contribution of International bodies like OECD, GDPR, ISO, ITU etc.,' likely delves into the roles and impacts of global organizations and frameworks in regulating, standardizing and shaping

international practices across sectors.

3. The fourth chapter, titled 'India's legal framework governing AI and Digital Trade,' explores the current policies, regulations, and legal developments in India surrounding Artificial Intelligence (AI) and digital commerce.
4. The fifth chapter, titled 'Towards Harmonized regulation of AI in Global Trade,' discusses the need, challenges, and prospects for establishing uniform regulatory framework for artificial intelligence (AI) in the context of international trade. Also, this chapter would address the key issues of harmonization across jurisdiction and the implication for global trade dynamics. This final chapter is likely to synthesizes the key insights from the preceding discussions and outlines actionable recommendations for stakeholders, policymakers, and international bodies.
5. Finally, the researcher has concluded the current study by emphasizing the critical need for a collaborative and forward-looking approach to address the challenges and opportunities posed by the evolving landscape of AI and global trade.

***

CHAPTER 2

Regulatory Landscape of AI in Global Trade

2.1 Introduction

Artificial intelligence (AI) is revolutionizing global trade, enhancing supply chain management, cross-border transactions, and market predictions. However, its integration into international commerce presents serious regulatory challenges. Liability attribution for AI-caused trade errors, biases in automated decision-making systems, and a lack of coherent global standards create legal uncertainty. This chapter critically examines the fragmented regulatory landscape surrounding AI in global trade and proposes solutions centered on transparency, accountability, and fairness.

2.2 AI in Global Trade: An Overview

Artificial Intelligence (AI) technologies are increasingly shaping the landscape of global trade by enhancing efficiency, reducing operational costs, and optimizing decision-making across borders. Their integration into the international trade ecosystem encompasses various applications, each bringing significant transformation but also introducing new complexities.

Applications:

1. **Smart Logistics**

   AI-powered logistics use predictive algorithms to optimize shipping routes, anticipate delays, and reduce delivery times[2]. By analyzing historical shipping data, weather conditions, port congestion, and even geopolitical risks, AI systems can reroute cargo dynamically, enhancing supply chain resilience.[3]

[2] Elgar Hofmann & Matthias Rüsch, *Industry 4.0 and the Current Status as Well as Future Prospects on Logistics*, 89 COMPUT. IND. 23 (2017), https://doi.org/10.1016/j.compind.2017.04.002. (Last visited on Jan 24, 2025)

[3] Dmitry Ivanov & Alexandre Dolgui Dmitry Ivanov & Alexandre Dolgui, *A Digital Supply Chain Twin for Managing the Disruption Risks and Resilience in the Era of Industry 4.0*, 142 TRANSP. RES. PART E: LOGISTICS & TRANSP. REV. 102190 (2020), https://doi.org/10.1016/j.tre.2020.102190. (Last visited on feb 2, 2025)

2. **Automated Customs Clearance**

   Customs procedures, traditionally paperwork-heavy and prone to delays, are being streamlined through AI. Automated systems can classify goods, detect anomalies, and even predict inspection needs based on learned patterns.[4] This not only reduces processing time but also minimizes human error and opportunities for corruption[5].

3. **AI-Driven Market Intelligence**

   By processing vast datasets—including news, social media, and trade records—AI tools can offer real-time insights into market trends, demand forecasts, and competitor behavior.[6]. These insights are invaluable for businesses navigating volatile international markets and formulating data-backed trade strategies.[7]

4. **Blockchain-AI Integration for Trade Finance**

   AI enhances blockchain applications in trade finance by verifying transaction authenticity, identifying fraud patterns, and automating compliance checks.[8] This synergy fosters trust in decentralized systems while maintaining regulatory oversight and accelerating the trade financing process.[9]

Challenges and Risks:

While AI contributes to increased efficiency and transparency, it also brings a layer of technological and regulatory complexity. One of the major issues is algorithmic bias—when AI systems inadvertently reflect historical inequalities or discriminatory practices.[10]

---

[4] Ming Xu & Min Li, *Artificial Intelligence for Customs Inspection: A Review*, 166 EXPERT SYST. WITH APPLICATIONS 114061 (2021), https://doi.org/10.1016/j.eswa.2020.114061. (Last visited on, Feb 9. 2025)

[5] World Customs Org., *Study Report on Disruptive Technologies* (2020), https://www.wcoomd.org. (Last visited on Mar 10, 2025).

[6] James Manyika et al., *The Age of Analytics: Competing in a Data-Driven World*, McKinsey Glob. Inst. Rep. (2016).

[7] Ying Zhang & Yong Zhao, *Big Data Analytics for Cross-Border E-Commerce: Insights and Research Directions*, 38 ELEC. COM. RES. & APPLICATIONS 100897 (2019), https://doi.org/10.1016/j.elerap.2019.100897. (Last visited on Mar 10, 2025)

[8] Sadegh Saberi, Mohammad Kouhizadeh, Joseph Sarkis & Lejia Shen, *Blockchain Technology and Its Relationships to Sustainable Supply Chain Management*, 57 INT'L J. PROD. RES. 2117 (2019), https://doi.org/10.1080/00207543.2018.1533261. (Last visited on Jan 6, 2025)

[9] Imran Bashir, *Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications* (Packt Publ'g 2020).

[10] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publ'g Grp. 2016).

In global trade, this can manifest in unfair tariff classifications or unjustified shipment delays, particularly in jurisdictions with limited oversight mechanisms.

Moreover, multi-jurisdictional data governance creates friction. Different countries impose varying data privacy and AI accountability regulations, which can lead to conflicts when AI systems operate across borders.[11] A biased decision made in one jurisdiction might trigger legal consequences in another, complicating liability and compliance for multinational firms.[12]

2.3. Regulatory Challenges in AI-Enabled Trade

As Artificial Intelligence becomes deeply embedded in global trade systems, regulatory frameworks struggle to keep pace. The challenges surrounding liability, bias, and legal harmonization raise serious concerns for governments, businesses, and civil society.

2.3.1 Liability for AI-Related Trade Errors

When AI systems make critical errors in international trade—such as delaying shipments, misclassifying tariff codes, or breaching trade restrictions—the question arises: who is legally responsible?

1. Lack of Intent in AI Decisions Traditional legal doctrines, especially those in tort and criminal law, rely on the concept of *mens rea*—human intent or negligence.[13] Since AI lacks consciousness and intent, applying these doctrines becomes problematic. Courts often have no clear method for attributing responsibility when AI acts independently based on learned data.[14]
2. Product Liability and the "AI as Product" Debate Scholars and regulators question whether AI algorithms can be treated as products under product liability

[11] Christopher Kuner et al., *International Regulation of AI: Issues and Directions*, 10 INT'L DATA PRIVACY L. 323 (2020), https://doi.org/10.1093/idpl/ipaa012. (Last visited on Feb, 2025)
[12] Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter & Luciano Floridi, *The Ethics of Algorithms: Mapping the Debate*, 3 BIG DATA & SOC'Y 1 (2016), https://doi.org/10.1177/2053951716679679. (Last visited on Mar 4, 2025)

[13] Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* (Springer 2013).
[14] Giovanni Sartor, *Artificial Intelligence and Legal Responsibility*, 378 PHIL. TRANSACTIONS ROYAL SOC'Y A 20190363 (2020), https://doi.org/10.1098/rsta.2019.0363. (Last visited on Mar 8, 2025)

frameworks[15]. If so, then developers or vendors might be liable for defects. However, because AI systems are dynamic and evolve over time, identifying a single point of failure—like in traditional manufacturing defects—is more complex[16].

3. Cross-Jurisdictional Legal Conflicts AI-enabled trade operations often span multiple legal systems. If an autonomous customs clearance system misclassifies restricted goods, it is unclear whether the liability lies with the AI's creator (often in one country), the trader (in another), or the logistics provider (in a third).[17] This multiplies legal uncertainty in dispute resolution and enforcement.[18]

2.3.2 Biases in Automated Decision-Making

AI systems trained on historical trade data may unintentionally reflect and reinforce existing inequalities in the global trading system.

1. **Systemic Bias and Discriminatory Outputs**

   If historical data contains patterns of preference or exclusion (e.g., favourable processing for Western countries), AI may amplify these biases.[19] For example, machine learning models used in customs risk assessments may prioritize inspections for goods from developing countries, assuming higher fraud risk, without evidence.[20]

2. **Violation of WTO principles**

   Such discriminatory practices challenge the *Most-Favoured-Nation (MFN)* and *National Treatment* principles under the World Trade Organization (WTO)

---

[15] European Comm'n, *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust* (2020), https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en. (Last visited on Apr 10, 2025w)

[16] High-Level Expert Grp. on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, European Comm'n (2019).

[17] Brent Mittelstadt, *Principles Alone Cannot Guarantee Ethical AI*, 1 NATURE MACHINE INTELLIGENCE 501 (2019).

[18] Lokke Moerel & Corien Prins, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things* (2016) (unpublished manuscript), https://ssrn.com/abstract=2784123.

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

[20] Andrew G. Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (N.Y.U. Press 2017).

framework, which require countries to treat all trading partners equally.[21] Biased AI decisions, even if unintentional, may constitute de facto discrimination in violation of international trade law.[22]

3. **Trade finance inequities**

   In the financial sector, trade finance algorithms may offer better loan terms to firms from high-income economies due to historical repayment patterns, thereby excluding SMEs in the Global South.[23] This replicates global inequalities and stifles inclusive trade development[24].

2.3.3 Fragmented Global Standards on AI

One of the most pressing challenges is the lack of harmonized international standards for AI regulation in trade contexts.

1. **European Union – EU AI Act**

   The EU's AI Act is a risk-based framework, categorizing AI systems based on the level of risk they pose to safety, rights, and livelihoods.[25] This Act is precautionary and mandates transparency, human oversight, and documentation for high-risk systems, such as those involved in border control or customs decisions.[26]

2. **United States – Sectoral and Light-Touch Regulation**

   The U.S. adopts a decentralized, sector-specific approach to AI governance. Agencies like the Federal Trade Commission (FTC) and Department of Commerce

---

[21] General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194 (Arts. I & III).
[22] Mira M. Wu, *The WTO and AI Governance: Discrimination, Transparency, and Surveillance*, 109 GEO. L.J. 263 (2021).
[23] Int'l Fin. Corp., Artificial Intelligence in Trade Finance: Current State and Future Outlook (2021), https://www.ifc.org. (Last visited on Jan 25, 2025)
[24] Sanae Ahmed & Andrei Zlate, *AI, Inequality, and Trade Finance Access in Developing Economies*, World Bank Pol'y Res. Working Paper No. 10108 (2022), https://documents.worldbank.org/en/publication/documents-reports/documentdetail/148321654530406662. (Last visited on Mar 22, 2025)
[25] European Comm'n, *Proposal for a Regulation on a European Approach for Artificial Intelligence (AI Act)*, COM (2021) 206 final (Apr. 21, 2021).
[26]Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, 22 COMPUTER L. REV. INT'L 97 (2021).

oversee particular domains but offer limited comprehensive guidance, prioritizing innovation over regulation[27].

3. **China – State-Centric Control Model**

   China enforces AI rules via a centralized, top-down regulatory system, emphasizing social stability, algorithm registration, and data localization.[28] These include mandatory security reviews and algorithm audits, particularly for platforms that impact public opinion or national security.[29]

4. **Consequences of Regulatory Divergence**

   For multinational traders, this regulatory fragmentation causes uncertainty, increases compliance costs, and poses risks of non-compliance across jurisdictions. It also hampers the development of interoperable AI systems, leading to inefficiencies and legal fragmentation in global supply chains.[30]

2.4. Current Legal Frameworks and Their Limitations

The rise of AI in global trade exposes significant regulatory blind spots in the existing legal infrastructure. While some international and regional frameworks have begun to address technological change, most remain ill-equipped to deal with the unique challenges AI presents in cross-border trade. These gaps span global institutions like the WTO, regional legal systems, and sector-specific oversight.

2.4.1 WTO Framework

The World Trade Organization (WTO) remains the backbone of multilateral trade governance, but its agreements were established long before AI became a trade issue.

1. No Clear Rules for AI-Based Trade Discrimination

   The WTO's rules on non-discrimination, embodied in the *Most-Favored-Nation* and *National Treatment* principles, prohibit treating foreign goods or services less

[27] Office of Sci. & Tech. Pol'y, *Blueprint for an AI Bill of Rights* (2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/. (Last visited on Jan 12, 2025)
[28] Elsa B. Kania, *China's AI Governance: Past, Present, and Future*, Ctr. for a New Am. Sec. (2020), https://www.cnas.org/publications/reports/chinas-ai-governance.
[29] Cyberspace Admin. of China, *Provisions on the Administration of Algorithmic Recommendation Services* (Mar. 1, 2022), https://www.cac.gov.cn/2022-01/04/c_1642894606682846.htm.
[30] Sophie de Moerloose & Thomas Cottier, Regulatory Fragmentation and International Trade in AI Technologies, 57 J. WORLD TRADE 49 (2023).

favorably[31]. However, AI-based systems can discriminate algorithmically, often unintentionally, and current rules do not recognize or regulate such digital forms of trade bias.[32]

2. No Liability Provisions for AI-Related Trade Disruptions

   The WTO lacks a liability framework for trade disruptions caused by autonomous or AI-driven systems. For instance, if an AI system blocks a legitimate trade transaction due to misclassification, there are no dispute mechanisms or liability clauses addressing technological error.[33]

3. No Digital Ethics or AI Principles in WTO Agreements

   Unlike emerging frameworks that incorporate ethics-by-design or trustworthy AI principles, WTO agreements do not address algorithmic transparency, explain ability, or fairness — concepts increasingly central to modern trade governance.[34]

2.4.2 Regional Initiatives

In response to global regulatory inertia, regional and national frameworks have begun to fill the governance vacuum—though with divergent philosophies and inconsistent scope.

1. European Union (EU): Draft Artificial Intelligence Act (2021)

   The EU AI Act adopts a risk-based approach, imposing the strictest requirements on "high-risk" applications, including AI used in customs, immigration, and financial services[35]. Obligations include data governance, documentation, human oversight, and auditability[36]. However, the act is still under negotiation and does not address cross-border liability or WTO harmonization.

2. United States: NIST AI Risk Management Framework (2023)

---

[31] World Trade Organization (1994). *General Agreement on Tariffs and Trade (GATT)*, Article I & III.
[32] Wu, M., Digital Discrimination in Global Trade: Challenges and Remedies, 109 Geo. L.J. 263 (2021).
[33] Low, P., AI, International Trade Law and WTO Reform, Geneva Trade Platform Discussion Paper (2020).
[34] Aaronson, S. A., The WTO and Digital Trade Governance, CIGI Papers No. 250 (2021).
[35] European Commission, Proposal for a Regulation on Artificial Intelligence, COM (2021) 206 final (2021).
[36] Veale, M. & Borgesius, F. Z., Demystifying the Draft EU Artificial Intelligence Act, 22 Comput. L. Rev. Int'l 97 (2021).

The NIST AI RMF offers a voluntary, industry-driven approach aimed at promoting AI accountability, fairness, and reliability[37]. It encourages businesses to self-assess risk rather than adhere to binding standards, which critics argue creates regulatory gaps in sectors like international logistics and trade finance.[38]

3. China: State-Centric AI Regulation

   China's legal framework emphasizes national security, content control, and data localization. Recent AI provisions require algorithm registration, explain ability, and security audits, especially for platforms that affect public opinion or cross-border data flows[39]. However, the approach is state-centric and lacks transparency or appeal mechanisms for affected traders.[40]

2.4.3 Sector-Specific Regulations

While global and regional governance remains patchy, certain trade-critical sectors have introduced preliminary regulatory responses to AI integration.

1. Shipping – International Maritime Organization (IMO)

   The IMO acknowledges that autonomous maritime systems pose risks, including navigation errors and cybersecurity breaches.[41] While the organization has issued guidelines for Maritime Autonomous Surface Ships (MASS), it has not established binding rules for AI decision-making, leaving legal gray zones for port entry, liability, and insurance claims.[42]

2. Finance – Regulatory Oversight of Automated Cross-Border Transactions

   In financial trade, AI systems automate currency exchange, risk scoring, and transaction monitoring. Regulators such as the Financial Action Task Force (FATF) and national central banks focus on anti-money laundering (AML) and counter-

[37] NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0) (2023), https://www.nist.gov/itl/ai-risk-management-framework. (Last visited on Mar 11, 2025)
[38] West, D. M. & Allen, J. R., Turning Point: Policymaking in the Era of Artificial Intelligence (2020).
[39] Cyberspace Administration of China, Provisions on the Management of Algorithmic Recommendation Services (2022).
[40] Kania, E., China's AI Regulations and the Global AI Race, Centre for a New American Security (2020).
[41] IMO, Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS) (2021).
[42] Fennelly, K. & FitzGerald, A., AI in Maritime Law: Liability Challenges, 53 J. Maritime L. & Com. 285 (2022).

terrorism financing (CTF), often ignoring broader algorithmic discrimination and fairness issues[43]/[44].

3. Compliance Limitations

   Most sector-specific efforts lack interoperability with international rules or one another. The result is a fragmented compliance environment, where multinational companies face inconsistent expectations across domains like shipping, payments, and customs.[45]

2.5. Case Studies

Case studies reveal the practical consequences of deploying AI in global trade, shedding light on compliance risks, systemic biases, and regulatory blind spots. These examples demonstrate how automation, when unchecked, can lead to violations of international trade norms and ethical principles.

2.5.1 AI and Cross-Border E-Commerce Disputes

E-commerce giants like Amazon and Alibaba rely heavily on AI-driven algorithms to manage millions of product listings and transactions daily. However, this automation can inadvertently violate trade sanctions or export control regulations when lacking human supervision.

1. Automated Listings and Sanctions Violations

   Both companies have encountered incidents where AI systems allowed the listing of prohibited or restricted items, such as military-grade equipment, dual-use goods, or products subject to U.S. and EU sanctions.[46] For instance, Amazon was fined by

[43] FATF, Opportunities and Challenges of New Technologies for AML/CFT (2021), https://www.fatf-gafi.org. (Last visited on May 2, 2025)
[44] Buckley, R. P., Arner, D. W. & Zetzsche, D. A., Fintech and Financial Inclusion: AI Regulation for Trade Finance, 22 J. Banking Reg. 1 (2021).
[45] De Moerloose, S. & Cottier, T., Regulatory Fragmentation and International Trade in AI Technologies, 57 J. World Trade 49 (2023).
[46] Hofmann, E. & Rüsch, M., Industry 4.0 and the Current Status as well as Future Prospects on Logistics, 89 Computers Ind. 23 (2017), https://doi.org/10.1016/j.compind.2017.04.002. (Last visited on April 7, 2025)

the U.S. Department of the Treasury for selling goods to sanctioned individuals and entities — an oversight attributed to its automated vetting system.[47]

2. Alibaba's Export Control Breaches

   Alibaba faced scrutiny for listings of surveillance technology and semiconductors possibly destined for prohibited jurisdictions, raising concerns about inadequate export screening mechanisms.[48] Automated systems failed to flag red flags due to lack of semantic understanding of nuanced compliance laws.

3. Legal and Financial Consequences

   These lapses expose companies to significant penalties under regimes such as the U.S. Office of Foreign Assets Control (OFAC), EU export control rules, and China's Export Control Law. The cases underscore the need for human-in-the-loop oversight in AI-driven compliance systems.[49]

2.5.2 Automated Customs and Bias Challenges

Customs authorities worldwide are integrating AI systems for risk-based targeting—flagging shipments for inspection based on predictive analytics. However, when trained on historically biased data, these systems may disproportionately target shipments from certain countries or regions.

1. Systemic Bias in Risk Algorithms

   AI models often use prior inspection outcomes, shipping origins, and trader behavior to flag high-risk cargo. However, if past inspections were biased against certain regions (e.g., Africa or Latin America), the model learns to repeat and perpetuate these patterns[50]. This results in more frequent inspections, longer delays, and increased trade costs for affected exporters.

---

[47] Ivanov, D. & Dolgui, A., A Digital Supply Chain Twin for Managing the Disruption Risks and Resilience in the Era of Industry 4.0, 142 Transp. Res. Part E 102190 (2020), https://doi.org/10.1016/j.tre.2020.102190. (Last visited on Feb 6, 2025)

[48] Xu, M. & Li, M., Artificial Intelligence for Customs Inspection: A Review, 166 Expert Sys. with Apps. 114061 (2021), https://doi.org/10.1016/j.eswa.2020.114061. (Last visited on May 2, 2025)

[49] World Customs Organization, Study Report on Disruptive Technologies (2020), https://www.wcoomd.org/. (Last visited on April 22, 2025)

[50] Manyika, J. et al., The Age of Analytics: Competing in a Data-Driven World, McKinsey Global Institute Report (2016).

2. Violation of WTO Fairness Principles

   Under WTO law, particularly Articles I and III of the General Agreement on Tariffs and Trade (GATT), all trading partners must be treated equally — a principle known as Most-Favored-Nation (MFN).[51] Biased AI targeting contradicts this by introducing de facto discrimination, even without intent.

3. Real-World Instances

   In 2020, reports emerged of automated customs screening systems in the EU and U.S. flagging disproportionately high volumes of shipments from African nations, prompting calls for algorithmic audits and transparency.[52] These systems often lacked explain ability features, making it hard for traders to challenge or understand why shipments were delayed.

4. Calls for Reform

   International organizations, including the World Customs Organization (WCO), have recommended guidelines for ethical AI use in customs, urging states to conduct bias impact assessments and provide appeal mechanisms for flagged shipments[53].

Challenges and Risks:

While AI contributes to increased efficiency and transparency, it also brings a layer of technological and regulatory complexity. One of the major issues is algorithmic bias—when AI systems inadvertently reflect historical inequalities or discriminatory practices[54]. In global trade, this can manifest in unfair tariff classifications or unjustified shipment delays, particularly in jurisdictions with limited oversight mechanisms.

Moreover, multi-jurisdictional data governance creates friction. Different countries impose varying data privacy and AI accountability regulations, which can lead to conflicts when

---

[51] Zhang, Y. & Zhao, Y., Big Data Analytics for Cross-Border E-Commerce: Insights and Research Directions, 38 Electron. Com. Res. & Apps. 100897 (2019), https://doi.org/10.1016/j.elerap.2019.100897. (Last visited on Feb 15, 2025)

[52] Saberi, S., Kouhizadeh, M., Sarkis, J. & Shen, L., Blockchain Technology and Its Relationships to Sustainable Supply Chain Management, 57 Int'l J. Production Res. 2117 (2019), https://doi.org/10.1080/00207543.2018.1533261. (Last visited on Jan 20, 2025)

[53] Bashir, I., Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications (2020).

[54] O'Neil, C., Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (2016).

AI systems operate across borders.[55] A biased decision made in one jurisdiction might trigger legal consequences in another, complicating liability and compliance for multinational firms.[56]

2.6. The Need for Global Standards

As Artificial Intelligence (AI) becomes integral to international trade operations—from customs clearance to trade finance—there is a pressing need for harmonized global standards that ensure transparency, accountability, and fairness. Without these, AI deployment can undermine the legitimacy of international commercial systems, create liability vacuums, and entrench global inequalities.

2.6.1 Transparency

Transparency refers to the explain ability and traceability of AI systems—especially those that affect regulatory or commercial decisions across borders.

1. Explainable Decision-Making

   For AI systems to be trusted in global trade, they must answer core questions:

   - *How was a decision made?*
   - *What data was used to arrive at it?*
   - Opaque systems that make "black box" decisions—especially in sensitive areas like customs, finance, or risk scoring—can lead to arbitrary outcomes, eroding trust among trade partners[57].

2. Importance in International Contexts

   In cross-border commerce, traders and governments must be able to understand and contest decisions. For example, why a particular shipment was flagged or why a financial transaction was denied. Without clear explanations, parties cannot exercise legal recourse or challenge biased or erroneous outcomes.[58]

---

[55] Kuner, C. et al., International Regulation of AI: Issues and Directions, 10 Int'l Data Privacy L. 323 (2020), https://doi.org/10.1093/idpl/ipaa012.
[56] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S. & Floridi, L., The Ethics of Algorithms: Mapping the Debate, 3 Big Data & Soc'y (2016), https://doi.org/10.1177/2053951716679679. (Last visited on Feb 2)
[57] Burrell, J., How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms, 3 Big Data & Soc'y 1 (2016), https://doi.org/10.1177/2053951715622512. (Last visited on Jan 16, 2025)
[58] Ananny, M. & Crawford, K., Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability, 20 New Media & Soc'y 973 (2018).

3. Global Efforts Toward Transparency

   Transparency is a core principle in the EU AI Act, which mandates that users of high-risk AI systems must be informed about the logic and functionality of the system[59]. Likewise, the OECD AI Principles advocate for *robust transparency and traceability* to support accountability.[60]

2.6.2 Accountability

Accountability ensures that there is a clearly identifiable party responsible when AI causes harm, makes a mistake, or violates laws in global trade contexts.

1. Assignment of Responsibility

   AI systems may involve multiple actors: developers, traders, platform providers, and logistics services. A well-defined framework must clarify:

   - *Who bears liability for AI errors (e.g., misclassification of goods)?*
   - *What legal mechanisms exist for redress?*[61]

     Without this, accountability becomes diffuse or non-existent, especially when the AI operates autonomously across jurisdictions.

2. Legal Complexity in Cross-Border AI Use

   Global trade involves intersecting national laws, which complicates jurisdiction and enforcement. For instance, if an AI-driven customs platform built in one country causes a delay in another, which country's courts have authority? This legal ambiguity often leaves injured parties without adequate remedies.[62]

3. Emerging Models

   The OECD AI Framework, and the UNCTAD Digital Economy Reports, stress the need for *shared international mechanisms* to handle liability, particularly in cross-border digital services and trade[63]/[64].

---

[59] European Commission, Proposal for a Regulation on Artificial Intelligence (EU AI Act), COM (2021) 206 final (2021).
[60] OECD, Recommendation of the Council on Artificial Intelligence (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. (Last visited on April 21, 2025)
[61] Pagallo, U., The Laws of Robots: Crimes, Contracts, and Torts (2013).
[62] Moerel, L. & Prins, C., Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data, SSRN Working Paper (2016).
[63] OECD, Framework for the Classification of AI Systems (2021).

2.6.3 Fairness

Fairness mandates that AI systems used in trade do not reinforce historical inequities, nor introduce new forms of discrimination against certain regions, businesses, or population groups.

1. Preventing Algorithmic Discrimination

   AI systems trained on skewed or biased data—such as customs records or trade finance outcomes—may favor exporters from wealthier countries while subjecting developing countries' shipments to heightened scrutiny[65]. This reproduces global trade disparities under the guise of automation.

2. Embedding Fairness in Trade Agreements

   Fairness needs to be codified into trade law, much like traditional non-discrimination principles in WTO rules. Future trade agreements should include:

   - *AI fairness clauses,*
   - *Obligations for algorithmic audits,*
   - *Rights to appeal AI-based decisions.*[66]

     Such measures can ensure AI does not become a digital barrier to trade.

3. WTO and Global Inclusion

   As of now, WTO law does not explicitly regulate AI-based discrimination. However, scholars argue for updating GATT and GATS provisions to cover digital fairness, ensuring equitable treatment in AI-mediated trade interactions.[67]

.

2.7. Proposed Regulatory Approaches

In response to the emerging risks and regulatory gaps of AI in global trade, scholars and policymakers have proposed multi-level interventions that span international treaties, certification systems, and financial instruments. These mechanisms aim to standardize rules, mitigate risk, and foster trust.

---

[65] Eubanks, V., Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2018).
[66] Wu, M., The WTO and AI Governance: Discrimination, Transparency, and Surveillance, 109 Geo. L.J. 263 (2021).
[67] Aaronson, S. A., Trade and the Governance of AI: WTO Blind Spots and the Need for Reform, CIGI Paper No. 256 (2021).

2.7.1 International AI Trade Treaty

A WTO-led multilateral treaty focused specifically on AI in trade could provide a foundational framework to address current legal and operational inconsistencies.

1. Harmonizing Liability Rules

   Such a treaty could clarify who is responsible when AI systems malfunction in cross-border operations (e.g., errors in automated customs or trade finance). This would reduce forum shopping and legal uncertainty.[68]

2. Mandating Transparency Requirements

   Transparency obligations—including explainability, traceability, and documentation of AI decisions—would promote predictability and contestability in global trade.[69]

3. Minimum Standards for Human Oversight

   By requiring human review in high-risk trade AI systems, the treaty could ensure accountability and ethical safeguards, aligning with the EU's approach in the AI Act.[70]

4. Precedents and Viability

   Precedents such as the WTO Trade Facilitation Agreement and Information Technology Agreement (ITA) show that plurilateral frameworks on technology and trade are possible.[71]

2.7.2 Ethical AI Certification Systems

A third-party certification model, similar to ISO standards, could establish baseline trust and interoperability for AI systems used in trade.

1. Bias-Free and Fair

[68] Low, P., AI, International Trade Law, and WTO Reform, Geneva Trade Platform (2020).
[69] Wu, M., The WTO and AI Governance, 109 Geo. L.J. 263 (2021).
[70] European Commission, Proposal for a Regulation on Artificial Intelligence, COM (2021) 206 final (2021).
[71] WTO, Trade Facilitation Agreement Overview (2017), https://www.wto.org/. (Last visited on Jan 23, 2025)

Certification agencies would verify that AI systems have undergone bias testing and fairness audits, essential for upholding WTO non-discrimination obligations[72].

2. Explain ability and Auditability

   AI systems would be required to maintain explainable logs and audit trails, allowing users and regulators to track decision-making paths[73].

3. Market and Diplomatic Benefits

   Certified AI systems would enjoy preferential recognition in customs and finance settings, fostering trust among trading partners and reducing barriers[74].

4. Model Examples

   Initiatives like IEEE P7003 (Algorithmic Bias Considerations) and AI Ethics Impact Group Certification in Germany provide early models for such schemes[75].

2.7.3 AI Liability Insurance Framework

The insurance sector could play a key role in absorbing and distributing risks arising from AI errors in trade logistics, documentation, or compliance.

1. Customized Coverage for AI Risks

   Insurance products can cover damages caused by autonomous systems in trade, such as misclassification of goods or contract breaches.[76]

2. Incentivizing Better Design and Governance

   Much like cyber insurance has improved organizational behavior, AI liability coverage would incentivize firms to use safer, well-documented, and certifiable AI tools.[77]

3. Global Precedents

---

[72] Eubanks, V., Automating Inequality (2018).
[73] Selbst, A. D. & Barocas, S., The Intuitive Appeal of Explainable Machines, 87 Fordham L. Rev. 1085 (2018).
[74] OECD, Trust in Trade in the Digital Age (2021).
[75] IEEE, P7003 - Algorithmic Bias Considerations Standard (2022), https://standards.ieee.org. (Last visited on Mar 4, 2025)
[76] Hacker, P. & Petkova, B., Reining in the Big Promise of Big Data, 15 Nw. J. Tech. & Intell. Prop. 3 (2017).
[77] Romanosky, S., Ablon, L., Kuehn, A. & Jones, T., Content Analysis of Cyber Insurance Policies, 5 J. Cybersecurity 1 (2019).

The European Commission and the OECD have both suggested insurance-backed models for AI accountability, especially in cross-border digital services.[78]

2.8. Role of International Organizations

Global governance of AI in trade cannot be achieved by individual countries alone. Multilateral organizations are instrumental in shaping rules, standards, and cooperative frameworks.

2.8.1 WTO and AI Regulations

The World Trade Organization (WTO) can play a transformative role in embedding AI governance into trade law.

1. Expanding the Work Programmed on E-Commerce
   Initially launched in 1998, this program can be updated to include AI-related trade issues, including algorithmic discrimination and customs automation.[79]
2. Negotiating AI Clauses in Trade Agreements
   As the WTO moves toward new plurilateral initiatives (e.g., the Joint Statement Initiative on e-commerce), it could embed rules on AI ethics, data flows, and liability[80].
3. Facilitating Dispute Resolution for AI-Related Trade Conflicts
   WTO panels may be equipped to handle AI-based trade discrimination cases, particularly if frameworks evolve to recognize algorithmic bias as a barrier[81].

2.8.2 OECD AI Principles

The OECD AI Principles, endorsed by 46 countries, provide a globally recognized ethical framework for trustworthy AI.

1. Core Pillars

[78] European Commission, AI White Paper, COM (2020) 65 final (2020).

[79] WTO, Work Programme on Electronic Commerce (1998).
[80] WTO, Joint Statement Initiative on E-Commerce (2021).
[81] Wu, M., Digital Trade and Algorithmic Discrimination, 109 Geo. L.J. 263 (2021).

These principles emphasize human-centered values, transparency, accountability, robustness, and inclusiveness[82].

2. Relevance to Trade

   By applying these principles to trade-related AI, governments can build interoperable frameworks and support fair digital commerce[83].

3. Policy Alignment

   The principles serve as a foundation for legislation like the EU AI Act and influence other multilateral dialogues such as the G7 AI Code of Conduct[84].

2.8.3 UN Initiatives

The United Nations, through various arms like the UN Secretary-General's office and UNCTAD, advocates for equitable and inclusive digital governance, including AI.

1. UN Digital Cooperation Roadmap

   This roadmap promotes multi-stakeholder dialogue and inclusive governance of digital technologies, with AI governance flagged as a key future frontier[85].

2. UNCTAD's Role in Trade and Technology

   The United Nations Conference on Trade and Development (UNCTAD) has emphasized AI's role in reshaping supply chains, services trade, and cross-border data governance.[86]

3. Prospect for UN-Led Frameworks

   With global legitimacy and convening power, the UN could help craft a universal treaty on AI ethics in trade, akin to UNESCO's 2021 *Recommendation on the Ethics of AI.*[87]

---

[82]OECD, OECD Principles on Artificial Intelligence (2019), https://www.oecd.org/going-digital/ai/principles/. (Last visited on Dec 27, 2025)
[83] OECD, Digital Economy Outlook (2021).
[84] G7, Hiroshima Process on Generative AI – Code of Conduct (2023).
[85] United Nations, Roadmap for Digital Cooperation (2020), https://www.un.org/en/digital-cooperation-roadmap. (Last visited May 2, 2025)
[86] UNCTAD, Digital Economy Report (2021).
[87] UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021), https://unesdoc.unesco.org/ark:/48223/pf0000381137. (Last visited May 3, 2025)

2.9. Conclusion and Future Prospects

The integration of Artificial Intelligence (AI) into global trade is no longer speculative—it is a rapidly unfolding reality. AI systems are already transforming logistics, customs, trade finance, compliance, and e-commerce at an unprecedented scale. However, this technological momentum is unfolding within a fragmented, inconsistent, and underdeveloped regulatory landscape.

The Inevitable Expansion of AI in Trade

AI is reshaping supply chain optimization, real-time decision-making, and risk mitigation across international commerce[88]. Its ability to process vast amounts of data and make rapid decisions promises transformative efficiencies, particularly in cross-border logistics, tariff classification, and automated compliance verification[89]. As AI adoption increases, interconnected global systems will become dependent on algorithms—making governance even more urgent.

Fragmentation in Global Regulation

Despite the growing reliance on AI, there is no unified regulatory framework to govern its use in trade. Countries and regions adopt divergent standards:

- The EU AI Act imposes strict risk-based regulations[90].
- The U.S. emphasizes voluntary frameworks via NIST[91].
- China implements top-down state-centric controls[92].

This fragmentation creates legal uncertainty, hampers interoperability, and imposes compliance burdens on multinational enterprises. It also limits AI's potential as a tool for inclusive globalization, favoring jurisdictions with regulatory clarity or economic

[88] Ivanov, D. & Dolgui, A., A Digital Supply Chain Twin for Managing the Disruption Risks and Resilience in the Era of Industry 4.0, 142 Transp. Res. Part E 102190 (2020), https://doi.org/10.1016/j.tre.2020.102190. (Last visited May 3, 2025)
[89] Manyika, J. et al., The Age of Analytics: Competing in a Data-Driven World, McKinsey Global Institute Report (2016).
[90] European Commission, Proposal for a Regulation on Artificial Intelligence (EU AI Act), COM (2021) 206 final (2021).
[91] NIST, AI Risk Management Framework (2023), https://www.nist.gov/itl/ai-risk-management-framework. (Last visited May 3, 2025)
[92] Cyberspace Administration of China, Provisions on the Management of Algorithmic Recommendation Services (2022). *Recommendation Services*.

leverage[93].

The Call for International Cooperation

To harness AI's potential responsibly, urgent multilateral cooperation is needed. Institutions like the WTO, OECD, and United Nations must lead in:

- Creating harmonized rules for AI liability, transparency, and ethical use.
- Developing shared oversight mechanisms.
- Ensuring non-discrimination principles are embedded in digital trade governance[94].

Without a global rules-based framework, AI risks becoming a tool of protectionism, digital exclusion, and algorithmic bias in trade.

Risks of Inaction

If left unregulated, AI in trade could:

- Exacerbate discrimination through biased algorithms that disadvantage firms or regions[95].
- Trigger trade disputes, especially when AI-generated decisions violate WTO principles (e.g., Most-Favoured-Nation treatment or national treatment rules).[96]
- Entrench global inequalities, favouring wealthier nations with more data resources and technical capacity.[97]

These risks demand not only regulatory responses but cross-border cooperation, digital diplomacy, and capacity-building in the Global South.

The Opportunity Ahead: AI for Inclusive Trade

With thoughtful design and ethical governance, AI could help realize the WTO's vision of an open, fair, and rules-based international trading system:

- Transparency in algorithmic decisions could reduce corruption and arbitrariness in customs.

---

[93] Aaronson, S. A., Trade and the Governance of AI: WTO Blind Spots and the Need for Reform, CIGI Paper No. 256 (2021).
[94] OECD, Recommendation of the Council on Artificial Intelligence (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. (Last visited May 7, 2025)
[95] Eubanks, V., Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2018).
[96]Wu, M., The WTO and AI Governance: Discrimination, Transparency, and Surveillance, 109 Geo. L.J. 263 (2021)..
[97] UNCTAD, Digital Economy Report 2021: Cross-border Data Flows and Development (2021), https://unctad.org/webflyer/digital-economy-report-2021. (Last visited May 5, 2025)

- Accountability mechanisms could build trust and clarify redress paths for stakeholders.
- Fairness in AI design could democratize access to trade finance and supply chain participation.[98]

AI can be a catalyst for inclusive globalization—empowering small businesses, improving logistics in developing countries, and fostering more resilient supply chains.[99]

[98] OECD, Trust in Trade in the Digital Age (2021).
[99] IFC, Artificial Intelligence in Trade Finance: Current State and Future Outlook (2021), International Finance Corporation.

CHAPTER 3

Contribution of International Bodies like OECD, GDPR, ISO and ITU

3.1 Introduction

The accelerating integration of Artificial Intelligence (AI) into global economic systems presents both transformative opportunities and unprecedented regulatory challenges. As AI technologies increasingly influence areas such as international trade, customs automation, cross-border data flows, and financial services, the absence of unified international governance frameworks has become a critical concern. The cross-jurisdictional nature of AI deployment—where algorithms developed in one country make decisions affecting markets and legal rights in another—demands international coordination to ensure consistency, fairness, and accountability in global commerce.[100]

Given that AI systems often rely on vast datasets and complex decision-making processes, their deployment in trade-related functions (e.g., customs classification, credit scoring, sanctions compliance) introduces risks of bias, opacity, and legal fragmentation.[101] No single country can effectively regulate these risks in isolation, especially when decisions made by automated systems can violate trade rules, infringe on data privacy rights, or create discriminatory outcomes that conflict with international norms such as the WTO's Most-Favored-Nation (MFN) principle.[102] Consequently, there is growing recognition that international organizations and legal instruments must play a central role in shaping the norms, ethics, and liability structures governing AI in trade and other transnational applications.[103]

This chapter focuses on the contributions of key international bodies and frameworks in shaping the global regulatory environment for AI. These include:

---

[100] See *U.N. Secretary-General's Roadmap for Digital Cooperation*, at 16–18, United Nations (2020), https://www.un.org/en/digital-cooperation-roadmap. (Last visited March 19, 2025)

[101] See Jenna Burrell, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, 3 *Big Data & Soc'y* 1, 3–4 (2016).

[102] *General Agreement on Tariffs and Trade*, art. I, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194.

[103] See Sandra Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 *Int'l Data Priv. L.* 76, 79–82 (2017).

- The Organization for Economic Co-operation and Development (OECD), whose *Principles on Artificial Intelligence* are among the first globally endorsed frameworks for trustworthy AI;
- The General Data Protection Regulation (GDPR), enacted by the European Union, which sets a global benchmark for data protection and algorithmic accountability;
- The International Organization for Standardization (ISO), which is developing technical standards for AI safety, explain ability, and interoperability;
- The International Telecommunication Union (ITU), which addresses AI infrastructure, connectivity, and ethical alignment with the UN Sustainable Development Goals.

Each of these institutions represents a unique approach to regulation, standard-setting, or ethical framing, and their collective impact is critical in moving toward harmonized AI governance.

The objective of this chapter is threefold:

(1) to evaluate the substantive contributions of these bodies to global AI governance, (2) to examine their influence on international trade practices and legal harmonization, and (3) to identify gaps and opportunities for enhanced collaboration in future regulatory architectures.

3.2 OECD: Fostering Ethical AI and Global Trade Governance

The Organisation for Economic Co-operation and Development (OECD) has emerged as a leading actor in shaping global norms for the ethical use of Artificial Intelligence (AI). Recognizing the far-reaching implications of AI in economic, social, and cross-border trade systems, the OECD has promoted interoperable, voluntary principles that serve as a foundation for both domestic legislation and multilateral coordination.

3.2.1 The OECD AI Principles

In 2019, the OECD released the OECD Principles on Artificial Intelligence, which became the first intergovernmental AI policy framework formally adopted by over 40 countries[104].

[104] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (May 22, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

These principles aim to promote trustworthy, human-centred AI and consist of five key values-based and five recommendations for national policies:

- Transparency and Explain ability: AI systems should be understandable and traceable, ensuring that individuals affected by algorithmic decisions can understand how those decisions were made.[105]
- Accountability**:** Organizations and individuals involved in the development and use of AI must be held responsible for its outcomes, including negative trade or compliance effects.[106]
- Robustness and Safety**:** AI systems must be technically resilient and secure, especially in high-risk environments such as customs, border control, and logistics.[107]
- Fairness and Human-Centred Values**:** AI should respect human rights, democratic values, and ensure non-discrimination across national boundaries.[108]

These principles align strongly with trade governance goals, particularly the WTO's emphasis on fairness, transparency, and predictability in international trade**.**

3.2.2 Relevance to Trade and Cross-Border Data Flows

The OECD AI Principles have direct implications for digital trade policies and cross**-**border data governance, areas increasingly shaped by algorithmic systems.

First, customs and trade facilitation systems now employ machine learning to identify risky shipments or streamline low-risk cargo. Without transparency and accountability mechanisms, such tools may introduce algorithmic bias that contravenes WTO non-discrimination rules.[109] By encouraging explainable AI, the OECD supports regulatory clarity and trust among trade partners.

Second, as cross-border data flows become essential to supply chain optimization and trade finance automation, the OECD's principles guide countries in harmonizing data privacy,

[105] Id. at § 1.3 (Transparency and Explain ability).
[106] Id. at § 1.4 (Accountability).
[107] Id. at § 1.2 (Robustness, Security, and Safety).
[108] Id. at § 1.1 (Inclusive Growth, Sustainable Development, and Well-being).

[109] Margaret Wu, The WTO and AI Governance: Discrimination, Transparency, and Surveillance, 109 *Geo. L.J.* 263, 285–86 (2021).

usage, and AI deployment standards.[110] This is critical as divergent regulations—such as between the EU's GDPR and China's data localization laws—pose risks to the interoperability of trade-related AI systems.

The OECD also influences regional and multilateral trade negotiations, such as those under the Joint Statement Initiative on E-Commerce at the WTO, by promoting aligned digital standards and ethical AI frameworks.[111]

3.2.3 Implementation and Global Adoption

Though a soft-law instrument, the OECD AI Principles have achieved widespread adoption and influence beyond OECD member states, including G20 and ASEAN nations.[112]

- Countries such as Japan, Singapore, and Brazil have incorporated OECD-inspired language into national AI strategies.
- The G7 and G20 have explicitly referenced the OECD principles in communiqués and ministerial statements, embedding these ideas into broader digital economy and trade dialogues.
- International organizations including the World Bank, UNESCO, and the ITU have used the OECD framework as a foundation for AI risk management, ethical assessments, and regulatory capacity building in developing countries.[113]

Despite their non-binding status, the principles have gained credibility due to their consensus-driven development, multi-stakeholder involvement, and alignment with economic and trade policy concerns. This makes them a critical tool in creating a convergent, ethical AI regime that can support fair and rules-based global trade.

3.3 GDPR: Data Protection and AI Regulation in Trade

The General Data Protection Regulation (GDPR), enacted by the European Union in 2016 and enforceable from May 2018, represents one of the world's most influential legal

---

[110] OECD, *Data Governance for Growth and Well-being* 13–15 (2022), https://www.oecd.org/digital/data-governance.htm.
[111] WTO, *Joint Statement Initiative on E-Commerce* (2021), https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm. (Last visited March 22, 2025)
[112] OECD, *AI Policy Observatory: Country Snapshots* (2023), https://oecd.ai/en/country-snapshots.
[113] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, U.N. Doc. 41 C/Res. 15 (2021); ITU, *AI for Good Global Summit Reports* (2022).

frameworks governing data privacy and the use of automated systems, including Artificial Intelligence (AI).[114] While originally intended to safeguard individuals' personal data, the GDPR has significant implications for global trade—particularly in sectors where AI systems process personal data for customs, logistics, consumer profiling, and cross-border transactions.

3.3.1 Overview of the GDPR Framework

The purpose of the GDPR is to provide individuals with control over their personal data while ensuring the free movement of such data within the European Union.[115] It establishes robust consent requirements**,** purpose limitation**,** and user rights over automated processing, thus creating a legal structure that affects AI applications deployed by both EU and non-EU entities[116].

One of the GDPR's most notable features is its extraterritorial scope, enshrined in Article 3**,** which applies the regulation to any organization—regardless of location—that offers goods or services to, or monitors the behaviour of, EU data subjects.[117] As such, a company in the United States or Asia using AI to optimize trade logistics or target EU customers through algorithmic profiling is still subject to the GDPR, including its rules on data minimization, automated decision-making, and cross-border transfers.

3.3.2 AI-Specific Provisions and Trade Implications

The GDPR includes specific provisions that directly affect how AI systems function in a trade context—particularly with regard to automated decision-making**,** profiling**,** and data economy practices**.**

- **Article 22** prohibits decisions based solely on automated processing—including profiling—that produce legal or similarly significant effects, unless the data subject has explicitly consented, the decision is necessary for a contract, or it is authorized

[114] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 O.J. (L 119) 1 [hereinafter GDPR].
[115] Id. art. 1(1).
[116] Id. arts. 5–6.
[117] Id. art. 3(2); see also Paul M. Schwartz, Global Data Privacy: The EU Way, 94 *N.Y.U. L. Rev.* 771, 777–80 (2019).

by Union or Member State law.[118] This is particularly relevant in AI-driven trade finance, credit assessment, or customs risk scoring systems, where decisions like loan approval or shipment detention are increasingly automated.

- **Article 5(1)(c)** establishes the principle of data minimization, requiring that data collected must be "adequate, relevant and limited to what is necessary" in relation to the purposes for which they are processed.[119] This challenges data-hungry AI systems often used in predictive analytics or demand forecasting, necessitating better data governance in AI design.

These provisions push developers and trade platform operators to design AI systems that are explainable, human-supervised, and rights-compatible, increasing compliance costs but also promoting ethical algorithm deployment in transnational commerce.

3.3.3 Compliance Challenges for Non-EU Traders

Non-EU businesses that deploy AI tools in cross-border trade or platform-based commerce frequently face operational difficulties complying with GDPR's requirements.

1. **Cross-border Data Transfers**: Under Chapter V of the GDPR, personal data may only be transferred to non-EU countries that ensure an adequate level of protection, as determined by the European Commission.[120] For AI vendors in countries without adequacy decisions—such as India, Brazil, or much of Southeast Asia—this restricts access to critical EU data needed for machine learning, analytics, or automation.
2. **Supply Chain AI and Logistics Automation**: Companies using AI for smart logistics, dynamic pricing, or fraud detection must build systems that can provide real-time explanations, consent management, and appeal processes, in line with GDPR safeguards[121]. This can be particularly burdensome for small and medium enterprises (SMEs) operating through digital platforms like Amazon, Alibaba, or Shopify.

---

[118] GDPR, supra note 1, art. 22.
[119] Id. art. 5(1)(c).
[120] Id. ch. V, arts. 44–45.
[121] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 *Int'l Data Priv. L.* 76, 79–81 (2017).

3. **Risk of Penalties and Trade Barriers**: Non-compliance can lead to substantial fines—up to 4% of global annual turnover under Article 83 of the GDPR.[122] Moreover, GDPR non-compliance may also be interpreted as a non-tariff barrier under international trade law, affecting the competitiveness of firms operating across digital borders.[123]

In sum, the GDPR is not just a privacy regulation; it is also an emerging digital trade standard—one that increasingly shapes how AI can be ethically and lawfully integrated into international commercial systems.

3.4 ISO: Global Standards for AI and Trade Technologies

The International Organization for Standardization (ISO), in collaboration with the International Electrotechnical Commission (IEC), plays a vital role in setting global technical and ethical standards for Artificial Intelligence (AI). These standards are instrumental in ensuring interoperability, safety, fairness, and trustworthiness of AI systems—key concerns in international trade, where automation and AI increasingly influence supply chains, logistics, compliance, and market access.

3.4.1 ISO/IEC JTC 1/SC 42 on Artificial Intelligence

The primary body within ISO responsible for AI standardization is ISO/IEC Joint Technical Committee 1, Subcommittee 42 (JTC 1/SC 42), established in 2018.[124] Its mandate is to develop foundational standards for AI, including terminology, governance frameworks, trustworthiness, and sector-specific applications.

SC 42 operates as a horizontal committee, meaning it does not regulate a specific industry but instead creates overarching standards that are applicable across verticals—including international trade and logistics.[125] It serves as a consensus-building platform, engaging stakeholders from over 50 countries and numerous liaison organizations, including IEEE, ITU, and the OECD.

---

[122] GDPR, supra note 1, art. 83(5).
[123] Anupam Chander & Uyen P. Le, Breaking the Web: Data Localization vs. the Global Internet, 61 *UCLA L. Rev.* 101, 135–138 (2014).
[124] ISO/IEC JTC 1/SC 42, *Artificial Intelligence*, Int'l Org. for Standardization (2023), https://www.iso.org/committee/6794475.html.

The committee's work supports alignment between national AI strategies and helps businesses design AI systems that are globally acceptable, which is essential for cross-border deployment in sectors like automated customs processing, trade finance, and e-commerce.

3.4.2 AI Risk Management, Bias Testing, and Transparency Standards

ISO/IEC JTC 1/SC 42 has developed a growing portfolio of standards that are directly relevant to global trade, particularly in managing risks and enhancing algorithmic transparency.

1. **ISO/IEC 23894:2023 – AI Risk Management**

   This standard provides a structured approach to identifying, assessing, and mitigating AI risks, especially for high-stakes applications in logistics, border control, and supply chain optimization.[126] It complements enterprise risk management systems and helps traders comply with emerging regulatory frameworks.

2. **ISO/IEC TR 24028:2020 – Trustworthiness in AI**

   This technical report outlines factors affecting the trustworthiness of AI systems, including accuracy, reliability, and safety—elements vital to ensuring that AI-driven trade processes are predictable and legally defensible.[127]

3. **ISO/IEC 12792 (Draft) – Bias in AI Systems and Datasets**

   This proposed standard aims to guide bias detection, measurement, and mitigation, a critical concern in trade where biased customs algorithms may lead to discriminatory treatment of goods or exporters.[128]

4. **ISO/IEC 38507:2022 – Governance of IT – Governance Implications of the Use of AI**

   This document helps organizations design AI governance structures, ensuring clear lines of responsibility, especially important in transnational supply chains where

[126] ISO/IEC 23894:2023, *Information Technology—Artificial Intelligence—Guidance on Risk Management*, Int'l Org. for Standardization (2023).
[127] ISO/IEC TR 24028:2020, *Information Technology—Artificial Intelligence—Overview of Trustworthiness in Artificial Intelligence*, Int'l Org. for Standardization (2020).
[128] ISO/IEC NP 12792, *Bias in AI Systems and Datasets*, Int'l Org. for Standardization (draft, under development).

liability for automated decisions must be established.[129] Together, these standards provide a non-binding but influential framework for building accountable, auditable, and trade-compliant AI systems.

3.4.3 Challenges in Adoption Across Jurisdictions

Despite their value, ISO standards face several barriers to widespread and uniform adoption in the international trade domain:

1. **Voluntary Nature of ISO Standards**

   ISO standards are non-mandatory unless incorporated into national law or contractual obligations.[130] This creates fragmentation in implementation, where businesses in some jurisdictions adopt strict AI design protocols while others do not, leading to inconsistencies in trade practices and compliance risks.

2. **Divergent National Approaches to AI Governance**

   Countries such as the EU (via the AI Act) and China (through sectoral regulations) impose state-centric or binding rules, while ISO remains technocratic and industry-driven, making coordination challenging[131]. The lack of harmonization increases costs for exporters who must meet different standards across regions.

3. **Resource Constraints in Developing Countries**

   ISO's complexity and technical language may exclude small firms and regulators in the Global South, who lack the capacity to integrate these standards into AI systems used for customs clearance, trade analytics, or fraud detection.[132] This deepens the digital divide in trade governance.

Despite these challenges, ISO/IEC JTC 1/SC 42 remains a cornerstone of efforts to create interoperable, safe, and fair AI systems for global commerce, and its work is increasingly informing both regulatory regimes and industry certification programs.

---

[129] ISO/IEC 38507:2022, *Governance of IT—Governance Implications of the Use of Artificial Intelligence*, Int'l Org. for Standardization (2022).
[130] Walter Mattli & Tim Büthe, *Setting International Standards: Technological Rationality or Primacy of Power?* 56 *World Pol.* 1, 17–21 (2003).
[131] European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM (2021) 206 final.
[132] UNCTAD, *Digital Economy Report 2021: Cross-border Data Flows and Development*, U.N. Doc. UNCTAD/DER/2021 (2021), https://unctad.org/webflyer/digital-economy-report-2021.

3.5 ITU: Telecommunication, AI Infrastructure, and Connectivity

The International Telecommunication Union (ITU), a specialized agency of the United Nations, plays a foundational role in setting global standards for telecommunications and emerging digital technologies, including Artificial Intelligence (AI).[133] As AI-driven systems rely heavily on connectivity, data infrastructure, and real-time transmission, ITU's work is instrumental in creating the enabling ecosystem for AI deployment in global trade. Beyond technical specifications, the ITU is increasingly focused on AI ethics, inclusion, and cross-border alignment, especially for developing economies. Through its AI for Good Global Summit and standards development efforts, the ITU promotes human-centered and sustainable uses of AI technologies across sectors, including trade facilitation, customs, smart logistics, and supply chain resilience.

3.5.1 ITU's AI for Good and Smart Trade Facilitation Initiatives

Launched in 2017, the AI for Good Global Summit serves as a multi-stakeholder platform bringing together governments, international organizations, academia, and private industry to explore ethical and development-focused applications of AI.[134] Among its key objectives is identifying how AI can be deployed to achieve the United Nations Sustainable Development Goals (SDGs)**,** many of which intersect with trade, such as decent work and economic growth**,** industry and infrastructure, and reducing inequality[135].

Within trade facilitation, the ITU has explored the use of AI in:

- Smart ports and customs automation**,**
- Real-time shipment tracking and forecasting**,** and
- Predictive risk analysis in cross-border logistics**.**

These initiatives aim to reduce friction in trade processes, particularly in regions with underdeveloped ICT infrastructure. Through collaboration with the World Customs

[133] Int'l Telecomm. Union [ITU], *Overview of the ITU and Its Mission*, https://www.itu.int/en/about/Pages/default.aspx
[134] ITU, *AI for Good Global Summit*, https://aiforgood.itu.int
[135] U.N. Dep't of Econ. & Soc. Affairs, *Sustainable Development Goals Report 2023*, https://unstats.un.org/sdgs/report/2023. (Last visited Feb 23, 2025)

Organization (WCO) and UNCTAD, the ITU supports AI-based systems that enhance supply chain visibility while safeguarding against digital exclusion.[136]

3.5.2 Technical Standards for AI Interoperability in Trade Systems

The ITU's Standardization Sector (ITU-T) develops technical specifications that ensure AI system interoperability, security, and scalability—prerequisites for effective deployment in cross-border trade environments. These standards provide the groundwork for aligning data flows, connectivity, and algorithmic protocols across national borders.[137]

Key initiatives include:

- **FG-AI4H (Focus Group on AI for Health)**: Though sector-specific, its frameworks for algorithm benchmarking and validation have informed discussions on AI quality assurance in trade finance and risk management**.**[138]
- **Recommendation ITU-T Y.3172**: Provides a framework for evaluating the trustworthiness of AI models, including criteria for robustness, fairness, and reliability in automated systems.[139]
- **AI and 5G/6G Synergies**: ITU works on ensuring that AI applications in smart logistics and customs clearance are optimized for low-latency, high-bandwidth environments made possible by 5G infrastructure.[140]

These standards support the technical backbone of digital trade, ensuring that different national systems can interoperate and comply with emerging AI governance norms.

3.5.3 ITU and Capacity Building in Developing Countries

One of the ITU's most critical contributions is its commitment to capacity building and digital inclusion, particularly in developing countries and least developed countries (LDCs) that risk marginalization in the AI-driven global economy.

---

[136] ITU, *AI and Trade Facilitation Case Studies*, in *AI for Good Reports*, https://aiforgood.itu.int/library (2022).
[137] ITU-T, *Artificial Intelligence – Overview of Activities*, https://www.itu.int/en/ITU-T/AI (2023).
[138] ITU & WHO, *Benchmarking AI Models for Health*, FG-AI4H Reports (2022), https://www.itu.int/en/ITU-T/focusgroups/ai4h.
[139] ITU-T Recommendation Y.3172, *Framework for Evaluating the Intelligence Level of Future Networks Including IMT-2020* (2021), https://www.itu.int/rec/T-REC-Y.3172.
[140] ITU-R, *IMT Vision Framework for 2030 and Beyond* (2023), https://www.itu.int/en/ITU-R/study-groups/rsg5/Pages/default.aspx.

Through its Digital Inclusion Programme and Partnership on Measuring ICT for Development, the ITU works to:

- **Bridge the digital divide** in trade-enabling infrastructure (e.g., customs digitization, e-commerce platforms),
- **Promote equitable access to AI technologies**, and
- **Support national AI policy development**, including through workshops and toolkits.[141]

The ITU's efforts in ensuring connectivity, affordability, and regulatory alignment are essential for enabling developing economies to participate in AI-enhanced global trade, without falling prey to digital colonialism or regulatory dependence.

3.6 Comparative Analysis of International Frameworks

The preceding sections have outlined how international institutions—the OECD**,** EU (via GDPR)**,** ISO/IEC**,** and ITU—approach Artificial Intelligence (AI) governance in the context of cross-border trade. This section offers a comparative analysis of their frameworks, focusing on three dimensions: (1) legal scope and binding force, (2) thematic focus and regulatory content, and (3) influence on national and transnational trade policy. While each framework contributes uniquely, they also expose gaps and inconsistencies that challenge harmonization in the global trade system.

3.6.1 Scope and Binding Nature

One of the most notable distinctions among these frameworks is their legal authority and enforceability.

- The GDPR is a legally binding regulation enacted by the European Union with extraterritorial reach, applying to all entities that process EU personal data, including those outside the EU.[142] It imposes specific obligations on algorithmic decision-making and data governance, with enforceable penalties for violations.[143]

[141] ITU, *Digital Inclusion: Bridging the Divide*, https://www.itu.int/en/ITU-D/Digital-Inclusion
[142] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 3.
[143] Id. art. 83.

- In contrast, the OECD AI Principles function as soft law—a non-binding but internationally endorsed set of norms.[144] They serve as aspirational guidance, lacking direct enforceability but exerting normative influence on domestic policymaking.
- **ISO standards** are voluntary technical frameworks, becoming mandatory only when incorporated into contracts or national laws.[145] Their role lies in standardizing implementation, not imposing policy obligations.
- The ITU offers a mix of technical recommendations (through ITU-T) and developmental programs, without binding force. However, it holds moral and strategic authority, especially in capacity-building contexts.[146]

This fragmented legal landscape creates challenges for businesses operating across jurisdictions, as AI compliance expectations may vary drastically depending on the region.

3.6.2 Areas of Overlap and Gaps

Despite their differences, these frameworks share common thematic pillars, particularly around trust, fairness, transparency, and accountability**:**

Framework	**Transparency**	**Accountability**	**Risk Management**	**Fairness/Non-Discrimination**
OECD	Strong[147]	Moderate[48]	General guidance[48]	Strong[48]
GDPR	Strong[148]	Legally binding[49]	Procedural[49]	Strong (via data subject rights)[49]
ISO	Technical[149]	Limited[50]	Detailed (e.g., ISO 23894)[50]	In progress (bias standards)[50]

[144] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[145] Walter Mattli & Tim Büthe, Setting International Standards: Technological Rationality or Primacy of Power? 56 *World Pol.* 1, 19–21 (2003).
[146] ITU, *AI for Good Global Summit*, https://aiforgood.itu.int (last visited May 19, 2025).
[147] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[148] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1, arts. 5, 22, 83.
[149] ISO/IEC 23894:2023, *Information Technology—Artificial Intelligence—Guidance on Risk Management*, Int'l Org. for Standardization (2023); ISO/IEC NP 12792, *Bias in AI Systems and Datasets* (draft); ISO/IEC 38507:2022.

ITU	Moderate[150]	Developmental[51]	Sectoral[51]	Embedded in SDG focus[51]

However, notable gaps remain:

- **Liability Frameworks**: Only GDPR provides clear mechanisms for assigning liability in the event of AI errors. Neither ISO nor OECD nor ITU explicitly addresses who is responsible when AI systems fail in international trade contexts[151].
- **Trade-Specific Provisions**: None of the frameworks (with partial exception of GDPR) tailor their standards specifically to trade facilitation**,** customs automation, or cross-border digital contracts**.**
- **Interoperability**: Differing terminology, compliance thresholds, and enforcement methods make interoperability across frameworks inconsistent, increasing compliance burdens for multinational enterprises[152].

3.6.3 Influence on Domestic Regulations and Trade Agreements

Each framework's influence on national laws and trade policy varies in scale and mechanism:

- The OECD AI Principles have been integrated into national strategies in countries such as Japan, Canada, and Singapore, and cited in policy dialogues including the G7 Hiroshima Process and WTO e-commerce negotiations**.**[153]
- The GDPR has inspired data protection regimes worldwide (e.g., Brazil's LGPD, California's CCPA), and increasingly functions as a global privacy benchmark—affecting how AI can be designed and deployed in trade systems.[154]

[150] ITU, *AI for Good Global Summit*, https://aiforgood.itu.int (last visited May 19, 2025); ITU-T Recommendation Y.3172, *Framework for Evaluating the Intelligence Level of Future Networks Including IMT-2020* (2021).
[151] Brent Mittelstadt, Principles Alone Cannot Guarantee Ethical AI, 1 *Nat. Mach. Intell.* 501, 505 (2019).
[152] Anupam Chander & Paul M. Schwartz, Privacy and/or Trade, 17 *Yale J.L. & Tech.* 121, 133–35 (2015).
[153] G7 Hiroshima Leaders' Communiqué, G7 Summit (May 2023), https://www.g7hiroshima.go.jp/documents/index.html.
[154] Graham Greenleaf, Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, 170 *Privacy Laws & Business Int'l Rep.* 1, 3–5 (2021)

- ISO standards underpin many public procurement frameworks and are being referenced in emerging AI certification schemes**,** such as those under the proposed EU AI Act.[155]
- The ITU**,** though less prescriptive, has steered AI infrastructure policy in Africa, Latin America, and Southeast Asia, aligning trade-enabling ICT systems with trust and equity principles embedded in the SDGs.[156]

Taken together, these frameworks shape the evolving architecture of AI governance in trade, yet their lack of cohesion presents serious risks to predictability, fairness, and scalability in global commerce.

3.7 Challenges and Critiques

Despite the contributions of international bodies like the OECD**,** GDPR (EU)**,** ISO**,** and ITU, the emerging landscape of AI governance remains riddled with systemic limitations that threaten to undermine consistency, fairness, and enforceability in cross-border trade applications. This section outlines the three most pressing challenges: regulatory fragmentation, implementation asymmetries, and overlapping or contradictory mandates.

3.7.1 Regulatory Fragmentation and Forum Shopping

One of the principal critiques of the current governance architecture is the lack of harmonization across jurisdictions, resulting in regulatory fragmentation**.** AI developers and multinational traders are frequently confronted with incompatible obligations:

- For example, the GDPR prohibits certain forms of automated profiling, while other jurisdictions (e.g., the U.S.) have no binding federal law on algorithmic fairness.[157]
- The EU AI Act, when finalized, will impose risk-tiered obligations that do not align with voluntary standards such as ISO or the soft-law principles of the OECD.[158]

---

[155] European Commission, *Proposal for a Regulation on Artificial Intelligence (EU AI Act)*, COM (2021) 206 final, art. 43.
[156] UNCTAD, *Digital Economy Report 2021: Cross-border Data Flows and Development*, U.N. Doc. UNCTAD/DER/2021, at 88–91.
[157] See GDPR, Regulation (EU) 2016/679, arts. 22–23, 2016 O.J. (L 119) 1; cf. U.S. Nat'l Inst. of Standards & Tech. [NIST], *AI Risk Management Framework* (2023), https://www.nist.gov/itl/ai-risk-management-framework. (Last visited on Jan26, 2025)
[158] European Commission, *Proposal for a Regulation on Artificial Intelligence (AI Act)*, COM (2021) 206 final.

This fragmentation encourages forum shopping, where firms choose to operate in jurisdictions with looser AI standards, undermining efforts to create a level playing field in international trade.[159] The absence of mutual recognition mechanisms across regimes further intensifies compliance burdens and legal uncertainty for businesses operating globally.

3.7.2 Implementation Disparities Between Global North and South

Another systemic critique is the unequal capacity of states to adopt, interpret, and enforce international AI norms. While OECD countries and regions like the EU have well-established data protection authorities, many developing countries lack technical expertise, financial resources, or institutional infrastructure to meaningfully engage with complex AI frameworks.[160]

This leads to a scenario where:

- **AI-enabled trade systems are disproportionately shaped by Global North standards**, and
- **Global South actors become rule-takers**, not rule-makers, in AI governance.[161]

Moreover, many international standards presume high levels of digital maturity, effectively excluding small and medium enterprises (SMEs) and customs authorities in developing nations from certification schemes or algorithmic audit processes.[162] Without inclusive design, the promise of AI to democratize trade becomes compromised.

3.7.3 Risk of Overlap, Redundancy, or Regulatory Chilling

Finally, there is increasing concern about overlapping mandates among international bodies. For instance:

---

[159] Anupam Chander, The Racist Algorithm? 115 *Mich. L. Rev.* 1023, 1044–45 (2017).
[160] UNCTAD, *Digital Economy Report 2021: Cross-border Data Flows and Development*, U.N. Doc. UNCTAD/DER/2021, at 89.
[161] Bukht, Rumana & Heeks, Richard, *Digital Economy and Development: Definitional Issues*, 5 *Dev. Informatics Working Paper* No. 68, 12 (2017).
[162] Eubanks, Virginia, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* 172–75 (2018).

- Both the OECD and ITU have issued AI guidelines rooted in fairness and transparency, but with different vocabularies, accountability scopes, and enforcement mechanisms**.**
- Similarly, the ISO's technical standards may contradict certain national policies if interpreted too rigidly, leading to regulatory chilling where businesses slow AI innovation to avoid future legal complications.[163]

Without better coordination, interoperability, and legal clarity, the simultaneous expansion of multiple standards can result in:

- **Redundancy**, where similar audits or certifications must be repeated across frameworks;
- **Conflict**, where one regime permits what another prohibits; and
- **Confusion**, especially for firms with cross-border digital operations.

Critics argue that a meta-governance mechanism—a higher-order coordinating framework—is urgently needed to synchronize these initiatives and preserve the functional integrity of international trade law in the digital era.[164]

3.8 Conclusion

The integration of Artificial Intelligence (AI) into global trade systems is both inevitable and transformative. From customs automation and smart logistics to AI-powered trade finance and cross-border data analytics, AI technologies are redefining the operational architecture of international commerce. Yet, this transformation also exposes profound regulatory, ethical, and technical challenges—particularly when AI is deployed without a clear, harmonized governance framework.

This chapter has examined the critical roles played by international bodies such as the OECD**,** European Union (via GDPR)**,** ISO/IEC, and the ITU in shaping global norms and standards for responsible AI. Each contributes uniquely:

[163] Brent Mittelstadt, Principles Alone Cannot Guarantee Ethical AI, 1 *Nat. Mach. Intell.* 501, 506–07 (2019).
[164] Floridi, Luciano et al., How to Design AI for Social Good: Seven Essential Requirements, 1 *Sci. & Eng'g Ethics* 20, 26–28 (2020).

- The OECD AI Principles have provided a soft-law foundation for trustworthy AI, influencing national strategies and multilateral dialogue.[165]
- The GDPR, while primarily a data protection law, imposes legally binding obligations on AI-driven systems and acts as a global reference point for algorithmic governance[166].
- The ISO/IEC JTC 1/SC 42 creates technical standards for risk management, transparency, and bias, critical for building trustworthy AI in trade operations[167].
- The ITU offers a connective infrastructure, focusing on interoperability, capacity-building**,** and ensuring equitable access to AI technologies, especially for developing countries.[168]

Despite these efforts, the current global framework is fragmented, uneven, and insufficient. There are:

- **Gaps in liability regimes** and mechanisms for enforcing accountability in cross-border AI trade disruptions;
- **Implementation asymmetries**, especially between the Global North and South, leading to disproportionate control and exclusion;
- And **overlapping mandates** among institutions, creating confusion for businesses and policymakers.[169]

The way forward lies in fostering institutional coordination and legal convergence. A potential solution could involve:

- Establishing a WTO-led plurilateral agreement on AI in trade, drawing from the OECD and ISO principles but giving them binding force in specific trade contexts;
- Encouraging interoperable certification schemes, grounded in ISO standards but enforced through GDPR-like accountability mechanisms;

---

[165] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[166] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1, arts. 5, 22.
[167] ISO/IEC 23894:2023, *Information Technology—Artificial Intelligence—Guidance on Risk Management*, Int'l Org. for Standardization (2023).
[168] ITU, *AI for Good Global Summit*, https://aiforgood.itu.int (last visited May 19, 2025).
[169] Brent Mittelstadt, Principles Alone Cannot Guarantee Ethical AI, 1 *Nat. Mach. Intell.* 501, 504–07 (2019).

- And enhancing multi-stakeholder dialogue through platforms like the ITU AI for Good Summit, ensuring inclusivity and knowledge-sharing.

Ultimately, with thoughtful international governance, AI has the potential to advance the WTO's vision of an open, inclusive, and rules-based trading system—rather than disrupt it. The challenge is not whether AI should shape global trade, but whether we can govern its integration ethically, fairly, and collaboratively.

Chapter 4

India's Legal Framework Governing AI and Digital Trade

4.1 Introduction

The rapid integration of Artificial Intelligence (AI) into global economies, coupled with the exponential growth of digital trade, has necessitated comprehensive legal and regulatory responses worldwide. In India, these developments have significant implications for national sovereignty, economic policy, data governance, and consumer protection. This chapter explores India's evolving legal framework that governs AI and digital commerce, focusing on the intersection of emerging technologies and law, and the regulatory architecture shaping this transformation.

India's position as a digital powerhouse—bolstered by government initiatives like Digital India and the National AI Strategy—has led to a growing reliance on AI in sectors such as healthcare, financial services, agriculture, e-commerce, education, and public administration.[170] With increasing AI adoption, legal questions surrounding data privacy, algorithmic bias, digital trade restrictions, and liability for AI-generated decisions have surfaced. In parallel, India's approach to digital trade—particularly its policy stance on data localization, cross-border data transfers, and digital taxation—reflects a balancing act between promoting innovation and protecting sovereign interests.

Scope

This chapter examines the legal and institutional landscape applicable to AI and digital trade in India, with a particular emphasis on key technologies like machine learning, automated decision-making systems, data analytics, and smart platforms. It also covers cross-border digital services such as fintech applications, cloud computing, and e-commerce platforms, which are increasingly dependent on AI-driven infrastructure. The discussion spans multiple sectors, including healthcare (telemedicine and diagnostics),

[170] *See generally* NITI Aayog, National Strategy for Artificial Intelligence – #AIforAll, https://www.niti.gov.in/sites/default/files/2021-07/NationalStrategy-for-AI-Discussion-Paper.pdf (last visited May 21, 2025).

financial technology (algorithmic trading, credit scoring), and online marketplaces (product recommendation algorithms and automated consumer redress systems).

The chapter evaluates regulatory frameworks developed or administered by core institutions such as the Ministry of Electronics and Information Technology (MeitY), the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the Telecom Regulatory Authority of India (TRAI), and newly proposed bodies like the Data Protection Board.[171] Judicial pronouncements, parliamentary committee reports, and policy white papers are also reviewed to understand legislative and administrative intent.

4.2 Overview of AI and Digital Trade in India

India's digital economy is undergoing a rapid transformation, driven by the integration of Artificial Intelligence (AI) and the expansion of digital trade. AI technologies—ranging from machine learning and computer vision to natural language processing and predictive analytics—are being deployed across diverse sectors. At the same time, digital trade is reshaping traditional commerce by enabling cross-border delivery of services, digital goods, and data flows. Understanding the scale, nature, and economic relevance of these trends is crucial to evaluating India's evolving legal and policy frameworks.

4.2.1 Defining AI and Digital Trade

Artificial Intelligence (AI) refers to computational systems capable of performing tasks that typically require human intelligence, including reasoning, learning, decision-making, and pattern recognition. AI technologies are often classified into:

- Narrow AI: Task-specific systems such as chatbots, recommendation engines, and fraud detection tools;
- General AI: Hypothetical systems with human-equivalent cognitive abilities.

Digital trade encompasses the digital delivery of goods and services, cross-border data flows, digitally-enabled transactions, and use of digital platforms in commerce.[172] The World Trade Organization (WTO) includes within digital trade elements such as cloud

[171] Ministry of Electronics & Information Technology, Digital Personal Data Protection Act, 2023, https://www.meity.gov.in/data-protection-framework (last visited May 21, 2025).

[172] Organisation for Economic Co-operation and Development, *Measuring the Digital Transformation: A Roadmap for the Future* (2019), https://www.oecd.org/going-digital/measuring-digital-transformation.pdf.

computing, digital content, software-as-a-service (SaaS), e-commerce platforms, and automated decision systems.[173]

In India, AI and digital trade are closely linked: AI systems often process data generated through digital platforms, enabling real-time decision-making, logistics optimization, dynamic pricing, and personalization of services.

4.2.2 India's AI Economy and Digital Infrastructure

India is currently among the top ten countries in terms of AI adoption and talent base, with over 4,000 start-ups and public-private AI initiatives across sectors.[174] According to NASSCOM, India's AI market is expected to grow to $7.8 billion by 2025, driven by investment in fintech, healthcare, agriculture, and retail.

Notable developments include:

- AI in governance: Facial recognition in policing, predictive analytics in welfare targeting;
- AI in health: Diagnostic tools, personalized medicine, pandemic response algorithms;
- AI in finance: Robo-advisors, credit-scoring systems, fraud detection;
- AI in retail/e-commerce: Automated supply chains, algorithmic pricing, behavioral targeting.

The Digital India program and expansion of national digital infrastructure—such as Aadhaar, UPI, and IndiaStack—have created a foundational ecosystem for AI deployment at scale.[175]

4.2.3 Sectoral Penetration and Economic Significance

AI technologies are now integral to multiple sectors of the Indian economy:

Sector	AI Applications

[173] World Trade Organization, *Work Programme on Electronic Commerce*, WT/L/274 (Sept. 1998), https://www.wto.org. (Last visited on April 28, 2025)
[174] NASSCOM, *AI Adoption in India: A Strategic Report*, 2023, https://nasscom.in.
[175] Ministry of Electronics & Information Technology, *Digital India: Empowering Citizens*, https://www.digitalindia.gov.in. (Last visited Apr 14, 2025)

Healthcare	AI diagnostics, remote triage, drug discovery[176]
Finance	Credit scoring, risk modelling, fraud detection[177]
E-Commerce	Personalization engines, chatbots, demand forecasting[178]
Agriculture	Crop prediction, smart irrigation, soil monitoring[179]
Education	Adaptive learning platforms, automated grading[180]
Public Services	Facial recognition, traffic management, grievance redressal[181]

India's AI Task Force, set up by the Ministry of Commerce and Industry, projects that AI could add up to $1 trillion to India's GDP by 2035 through productivity enhancements, innovation, and export growth.[182]

4.2.4 Governmental and Policy Frameworks

Several government bodies and strategic documents have guided India's AI journey:

[176] NITI Aayog, *National Strategy for Artificial Intelligence – #AIforAll* (2018), https://www.niti.gov.in/sites/default/files/2021-07/NationalStrategy-for-AI-Discussion-Paper.pdf. / Ministry of Health and Family Welfare, *Guidelines for Telemedicine in India* (2020), https://www.nmc.org.in/MCIRest/open/getDocument?path=/Documents/Public/Portal/LatestNews/Guidelines_for_Telemedicine_in_India.pdf.

[177] Reserve Bank of India, *Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps* (Nov. 2021), https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189. / Nasscom & BCG, *AI Adoption in Indian Enterprises* (2021), https://nasscom.in/knowledge-center/publications/ai-adoption-indian-enterprises.

[178] Nasscom & BCG, *AI Adoption in Indian Enterprises* (2021), https://nasscom.in/knowledge-center/publications/ai-adoption-indian-enterprises. / Ministry of Electronics and Information Technology (MeitY), *Responsible AI for Social Empowerment (RAISE 2020) Summit Report*, https://www.meity.gov.in.

[179] NITI Aayog, *National Strategy for Artificial Intelligence – #AIforAll* (2018), https://www.niti.gov.in/sites/default/files/2021-07/NationalStrategy-for-AI-Discussion-Paper.pdf. / Ministry of Agriculture and Farmers Welfare, *AI in Agriculture: Use Cases and Policy Suggestions*, Policy Brief No. 8 (2022), https://agricoop.nic.in. Last visited Feb 22, 2025)

[180] UNESCO, *AI and Education: Guidance for Policymakers* (2021), https://unesdoc.unesco.org/ark:/48223/pf0000376709. / NITI Aayog, *National Strategy for Artificial Intelligence – #AIforAll* (2018), https://www.niti.gov.in/sites/default/files/2021-07/NationalStrategy-for-AI-Discussion-Paper.pdf.

[181] Internet Freedom Foundation, *Project Panoptic: Facial Recognition in India* (2021), https://panoptic.in. / Ministry of Electronics and Information Technology (MeitY), *Responsible AI for Social Empowerment (RAISE 2020) Summit Report*, https://www.meity.gov.in. (Last visited Feb 24, 2025)

[182] Ministry of Commerce and Industry, *AI Task Force Report*, 2018, https://dpiit.gov.in.

- **NITI Aayog's National Strategy for AI (2018)** outlined core focus areas including healthcare, agriculture, education, smart mobility, and urban infrastructure.[183]
- **Digital India Program** aims to transform the country into a knowledge-based economy with digital access and inclusion.
- **MeitY's AI for All initiative** promotes responsible AI, ethical research, and skilling of the workforce.
- **National Data and Analytics Platform (NDAP)** and **AI Centers of Excellence** facilitate open data access and R&D.

However, many of these policies remain non-binding, and there is no dedicated AI legislation yet in place.

4.2.5 Cross-Border Digital Trade

India is a key player in the global digital trade ecosystem through its IT services exports, SaaS providers, and BPO sectors. The increasing reliance on data-intensive services, however, has brought regulatory tensions to the fore—particularly around:

- Data localization requirements;
- Restrictions on cross-border data flows;
- Algorithmic accountability in foreign digital platforms operating in India.

India has refrained from joining WTO's Joint Statement Initiative (JSI) on E-Commerce, citing the need to preserve digital policy space and safeguard national interest.[184] Nonetheless, the country is engaged in bilateral negotiations where digital trade and AI cooperation are emerging themes.

4.2.6 Interplay of AI, Trade, and Law

The convergence of AI and digital trade raises multi-dimensional legal questions:

- How should AI-generated content be taxed or protected under intellectual property law?

---

[183] NITI Aayog, *National Strategy for Artificial Intelligence – #AIforAll*, 2018, https://www.niti.gov.in. (Last visited Feb 2, 2025)

[184] Ministry of Commerce, *India's Position on WTO E-Commerce Discussions*, https://commerce.gov.in. (Last visited on Feb 25, 2025)

- What standards should apply to algorithmic decision-making across borders?
- Should data localization be mandated for AI model training or cloud deployment?
- How can India ensure interoperability with global legal frameworks while maintaining digital sovereignty?

4.3 Regulatory Institutions and Policy Bodies

The legal governance of Artificial Intelligence (AI) and digital trade in India is distributed across a range of institutions with overlapping mandates and responsibilities. As technological advancement outpaces regulatory evolution, institutional coordination and the development of a unified framework have become critical. This section explores the major regulatory bodies involved in AI and digital trade governance, highlighting their roles, contributions, and inter-agency dynamics.

4.3.1 NITI Aayog: Strategic Planning and Policy Vision

NITI Aayog has played a foundational role in conceptualizing India's national AI strategy. As the government's premier policy think tank, it published the National Strategy for Artificial Intelligence (#AIforAll), which emphasizes inclusive economic growth through the deployment of AI across priority sectors such as healthcare, agriculture, education, smart cities, and mobility.[185] While the strategy lacks binding legal authority, it serves as a key normative document guiding both central and state-level AI initiatives.

NITI Aayog has also piloted AI-based programs through collaborations with private sector stakeholders, indicating a preference for innovation sandboxes and public-private partnerships rather than immediate regulation.[186] However, critics argue that the absence of legislative force limits the practical enforceability and consistency of such strategic frameworks.

[185] NITI Aayog**,** National Strategy for Artificial Intelligence – #AIforAll**,** https://www.niti.gov.in/sites/default/files/2021-07/NationalStrategy-for-AI-Discussion-Paper.pdf (last visited May 22, 2025).

[186] Press Trust of India, NITI Aayog Collaborates with Oracle, Apollo Hospitals on AI-Powered Healthcare, *The Economic Times* (Feb. 28, 2018), https://economictimes.indiatimes.com.

4.3.2 Ministry of Electronics and Information Technology (MeitY)

MeitY is the central administrative authority responsible for formulating and implementing policies on information technology, including AI systems and digital commerce infrastructure. It oversees critical legislation such as the Information Technology Act, 2000 and the newly enacted Digital Personal Data Protection Act, 2023.[187]

MeitY has also initiated regulatory sandboxes, funded AI research centres, and convened public consultations on emerging technologies. It plays a central role in India's stance on data localization and cross-border data transfers, both of which directly affect AI development and digital trade agreements. MeitY's position reflects a policy tilt toward digital sovereignty, seeking to balance innovation with data security and citizen rights.[188]

4.3.3 Reserve Bank of India (RBI)

The RBI regulates the financial sector, including AI applications in fintech such as automated lending, algorithmic trading, and fraud detection. Through the creation of its regulatory sandbox framework in 2019, the RBI has permitted limited-scale testing of AI-driven financial services under regulatory oversight.[189] It has issued advisories on algorithmic credit scoring and the ethical use of AI in consumer financial services.

The RBI's digital currency initiatives and Unified Payments Interface (UPI) frameworks also create a digital infrastructure that underpins much of the AI-facilitated financial trade in India. Its regulatory oversight ensures systemic risk management and consumer protection in the use of AI for digital finance.

4.3.4 Securities and Exchange Board of India (SEBI)

SEBI regulates capital markets and has issued guidelines pertaining to the use of algorithmic trading and high-frequency trading—both of which rely heavily on AI

[187] Ministry of Electronics & Information Technology, Digital Personal Data Protection Act, 2023, https://www.meity.gov.in/data-protection-framework (last visited May 22, 2025).
[188] Press Information Bureau, MeitY Holds Public Consultation on Cross-Border Data Flows (July 20, 2023), https://pib.gov.in. (Last visited Feb 24, 2025)
[189] Reserve Bank of India, *Enabling Framework for Regulatory Sandbox* (Aug. 2019), https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11618&Mode=0 (last visited May 22, 2025).

models.[190] SEBI's focus has been on ensuring market transparency, fairness, and risk containment. It has mandated periodic reporting on the logic of AI models used in trading and emphasized the need for explain ability, particularly to mitigate systemic risks and market manipulation.

4.3.5 Telecom Regulatory Authority of India (TRAI)

As AI applications expand into telecommunications—especially in network optimization, fraud detection, and personalized advertising—TRAI plays a regulatory role in ensuring non-discrimination, consumer protection, and network neutrality.[191] TRAI has also explored AI's potential in enhancing public service delivery, such as through spectrum management and rural connectivity.

4.3.6 Data Protection Board (Proposed)

The Digital Personal Data Protection Act, 2023 establishes a Data Protection Board of India**,** tasked with adjudicating disputes and ensuring compliance with data protection norms.[192] While yet to be operationalized, this institution is expected to have significant influence over how data used in AI systems is collected, stored, and processed—particularly concerning cross-border data transfers, algorithmic decision-making, and data fiduciary obligations.

The Board is also expected to create binding guidance on anonymization standards and redress mechanisms, both of which are fundamental to ensuring ethical AI deployment.

4.3.7 Judiciary and Parliamentary Committees

Indian courts have begun grappling with digital rights issues in landmark cases such as *Justice K.S. Puttaswamy v. Union of India*, which recognized the right to privacy as a

[190] Securities and Exchange Board of India, *Framework for Algorithmic Trading by Mutual Funds* (2021), https://www.sebi.gov.in/legal/circulars/oct-2021/framework-for-algorithmic-trading-by-mutual-funds_53392.html.
[191] Telecom Regulatory Authority of India, *Recommendations on Artificial Intelligence and Big Data in Telecom Sector* (Apr. 2022), https://www.trai.gov.in/release-publication/reports.
[192] Digital Personal Data Protection Act, 2023, § 19, https://www.meity.gov.in/data-protection-framework.

fundamental right under Article 21 of the Constitution.[193] While not AI-specific, such decisions lay foundational principles that can guide future AI jurisprudence.

Parliamentary Standing Committees—such as the Committee on Information Technology and the Committee on Finance—have also conducted inquiries into digital platforms, algorithmic accountability, and competition in digital markets. These discussions are increasingly influencing legislative directions on AI governance.[194]

4.3.8 Inter-Agency Coordination Challenges

Despite the range of institutions involved, regulatory overlap and fragmentation remain key concerns. For example, both MeitY and RBI regulate digital payment systems involving AI, while TRAI and SEBI supervise algorithmic operations in overlapping domains like digital trading and telecom platforms. There is currently no central regulatory architecture or overarching AI law that harmonizes these efforts, which can lead to jurisdictional conflicts and inconsistent enforcement.

Establishing a National AI Regulatory Authority or formal inter-regulatory coordination mechanism has been proposed in various policy white papers but is yet to be implemented.

4.4 Existing Legal Frameworks Relevant to AI and Digital Trade

India does not currently have a standalone, comprehensive legislation dedicated solely to artificial intelligence (AI) or digital trade. Instead, the regulation of AI and digital commerce is governed by a patchwork of sectoral laws, rules, executive policies, and judicial interpretations. This fragmented legal framework creates both opportunities and limitations in addressing the risks and benefits of AI deployment and the facilitation of cross-border digital transactions. This section analyses key legislative instruments and their relevance to AI and digital trade in India.

4.4.1 The Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) forms the bedrock of India's digital legal

[193] *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India*, (2017) 10 S.C.C. 1 (India).
[194] Parliamentary Standing Committee on Finance, Report on Anti-Competitive Practices by Big Tech (Dec. 2022), https://loksabhadocs.nic.in.

infrastructure. Enacted to provide legal recognition to electronic transactions and cybercrime regulation, the IT Act has since evolved to cover broader aspects of data security, intermediary liability, and digital governance.[195] Although it does not mention AI explicitly, several of its provisions are indirectly relevant:

- **Section 43A** deals with compensation for failure to protect data, which may apply to AI systems that rely on large-scale personal data.
- **Section 66** criminalizes unauthorized access, data theft, and identity fraud—issues pertinent to AI-enabled platforms.[196]
- **Rules under Section 79** outline intermediary due diligence, relevant to AI-powered content recommendation systems on digital platforms.

Despite these provisions, the IT Act lacks any normative framework for governing algorithmic accountability, transparency, or ethical AI design. As AI systems begin making autonomous decisions, the absence of targeted provisions addressing explain ability or AI liability has become a regulatory gap.

4.4.2 The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's most recent and comprehensive effort to regulate personal data processing. While not AI-specific, its provisions profoundly affect AI operations, particularly regarding training data, profiling, and automated decision-making.[197]

Key features of the Act include:

- **Consent-based Data Processing**: All AI systems processing personal data must obtain verifiable user consent, impacting real-time data analytics and profiling functions.[198]

---

[195] Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India), https://www.meity.gov.in. (Last visited Jan 26, 2025)

[196] Ministry of Electronics and Information Technology, *Information Technology Rules (Intermediary Guidelines and Digital Media Ethics Code), 2021*, https://www.meity.gov.in/content/intermediary-guidelines.

[197] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India), https://www.meity.gov.in/data-protection-framework.

[198] Data Protection Board of India, FAQs on Consent, https://www.dpdp.gov.in/faqs (last visited May 22, 2025).

- **Obligations on Data Fiduciaries**: Entities deploying AI must ensure purpose limitation, data minimization, and user rights, such as access, correction, and grievance redressal.
- **Cross-Border Data Transfer**: The Act permits the government to notify "trusted" countries for data export, which influences AI models relying on global datasets.

While the Act improves transparency and user autonomy, it does not yet include a right to explanation found in other jurisdictions, such as the European Union's General Data Protection Regulation (GDPR).[199] This may weaken users' control over AI-based automated decisions in India.

4.4.3 Consumer Protection (E-Commerce) Rules, 2020

Issued under the Consumer Protection Act, 2019, the E-Commerce Rules, 2020 regulate online marketplaces, many of which deploy AI for product recommendations, dynamic pricing, and consumer redress mechanisms.[200]

Key obligations relevant to AI-based digital commerce include:

- **Liability Disclosure**: E-commerce platforms must disclose the parameters of algorithmic ranking and search prioritization.
- **Grievance Redressal**: Requirements to establish grievance officers for complaints against AI-driven practices like unfair pricing or discriminatory advertising.
- **Misleading Advertisements and Dark Patterns**: Regulation of AI-enabled advertising systems and algorithms that nudge users through behavioral manipulation.

Although the rules increase accountability, enforcement remains weak, especially concerning global platforms operating in India with proprietary AI algorithms.

4.4.4 Sector-Specific Regulations

In addition to general laws, several sectors in India have promulgated regulations that intersect with AI and digital trade:

---

[199] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119) 1 (General Data Protection Regulation).

[200] Consumer Protection (E-Commerce) Rules, 2020, Ministry of Consumer Affairs, https://consumeraffairs.nic.in.

- **Healthcare**: The Telemedicine Practice Guidelines, 2020, published by the Medical Council of India, permit remote consultations but are silent on AI-enabled diagnostics, creating ambiguity around medical liability for AI use in treatment decisions.[201]
- **Financial Services**: The Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) regulate algorithmic trading, credit scoring, and fraud detection. The RBI has issued sandbox frameworks for AI innovation, but broader systemic safeguards are still lacking.[202]
- **Education**: EdTech platforms using AI for personalized learning are largely unregulated, though the National Education Policy, 2020 recognizes the importance of ethical AI integration in education.[203]

4.4.5 Pending and Draft Frameworks

India is also considering a number of draft policies that could reshape the legal landscape for AI and digital trade:

- **Non-Personal Data Governance Framework**: The Committee of Experts chaired by Kris Gopalakrishnan recommended the regulation of anonymized datasets used in AI training, proposing mandatory data sharing for public benefit and innovation.[204]
- **National Cybersecurity Strategy**: Drafted by the National Security Council Secretariat, this strategy includes provisions for AI system resilience and threat detection capabilities, but it remains unpublished.

These frameworks highlight India's growing recognition of the need for comprehensive AI regulation but also underscore the lack of legislative finality.

---

[201] Medical Council of India, *Telemedicine Practice Guidelines* (Mar. 25, 2020), https://www.nmc.org.in.
[202]Reserve Bank of India, *Regulatory Sandbox Framework for FinTech*, https://www.rbi.org.in (Last visited on Apr 30, 2025)
[203]. Ministry of Education, *National Education Policy, 2020*, https://www.education.gov.in.
[204] Kris Gopalakrishnan Committee, *Report on Non-Personal Data Governance Framework*, Ministry of Electronics and Information Technology (Dec. 2020), https://www.meity.gov.in/writereaddata/files/NPD_Report_on_Non-Personal_Data_Governance_Framework.pdf.

4.5 Emerging AI-Specific Legal Challenges

While India has made significant progress in digital governance through statutes like the IT Act, the DPDP Act, and sector-specific regulations, these frameworks are still largely technology-neutral and reactive in nature. As AI systems become more autonomous, opaque, and embedded in economic decision-making, they present distinct challenges that require targeted legal responses. This section identifies and analyses the key AI-specific legal issues that remain underdeveloped in India's current framework.

4.5.1 Bias, Discrimination, and Fairness

Algorithmic bias poses a serious challenge to the equitable deployment of AI, especially in sensitive domains like credit scoring, recruitment, insurance, and criminal justice. Machine learning systems can inherit or amplify existing social, racial, gender, or economic prejudices embedded in training data, leading to discriminatory outcomes.

India currently lacks legal provisions mandating bias audits or algorithmic fairness assessments. Unlike the EU's AI Act, which classifies certain AI applications as high-risk and prescribes strict compliance mechanisms.[205] Indian law does not yet impose affirmative obligations on developers or deployers of AI to detect or mitigate discriminatory effects.

This regulatory vacuum has led to concerns about violations of constitutional rights, particularly Article 14 (equality before the law) and Article 21 (protection of life and personal liberty), when AI is used in public services or decision-making systems.[206]

4.5.2 Transparency, Explain ability, and the Right to Explanation

AI systems, particularly those based on deep learning or neural networks, often function as "black boxes," making it difficult for users or regulators to understand how specific decisions are made. This raises questions about the right to explanation, a principle that has found place in international legal frameworks such as the GDPR but remains absent in Indian law.[207]

---

[205] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final (Apr. 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206. (Last visited on Jan 21, 2025)

[206] Constitution of India, art. 14, 21.

[207] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119) 1.

Transparency obligations under India's DPDP Act require that data principals be informed of data use and purpose, but they do not extend to algorithmic logic or automated profiling. Without clear obligations on explain ability, individuals may have little recourse to challenge adverse decisions made by AI in areas like loan rejections, academic admissions, or insurance premiums.

Calls have been made by civil society groups and parliamentary committees for mandatory documentation and audit trails of AI decision-making, but these remain non-binding recommendations.[208]

4.5.3 Autonomy and Liability for AI-Generated Decisions

The autonomy of AI systems raises unresolved questions regarding legal liability**,** particularly when AI systems act without direct human intervention. Under current Indian tort and contract law, liability is generally premised on human agency. This raises complex issues when harm is caused by self-learning algorithms that evolve beyond their initial programming.

There is no settled doctrine in Indian jurisprudence on whether developers, data providers, or end-users should bear responsibility for AI-caused damage. Courts have also not yet developed standards to assess foreseeability or negligence in the context of algorithmic actions.

Comparative jurisdictions have considered assigning "electronic personality" to AI for the purposes of liability, but such approaches remain controversial and are not currently contemplated in India.[209] Regulatory certainty in this domain is crucial for industries deploying autonomous systems, such as self-driving vehicles or AI-powered diagnostic tools.

4.5.4 Data Sovereignty and Cross-Border Trade Barriers

India's emphasis on data localization and digital sovereignty has direct implications for cross-border digital trade and AI development. Many AI models require large, diverse

[208] Internet Freedom Foundation, *Submission to MeitY on Need for Algorithmic Transparency in AI Systems*, https://internetfreedom.in. (Last visited on Feb 12, 2025)

[209] European Parliament Resolution of 16 Feb. 2017 with Recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL), https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html. (Last visited Mar 23, 2025)

datasets for training, which may not be fully accessible if data is restricted to national boundaries. Provisions under the DPDP Act allow the central government to restrict cross-border data flows, subject to bilateral agreements and "trusted" nations lists.[210]

These restrictions may conflict with India's commitments under World Trade Organization (WTO) disciplines and proposed Free Trade Agreements (FTAs), particularly in digital services and e-commerce chapters. For example, India has refused to join the WTO's Joint Statement Initiative on E-commerce, citing concerns about regulatory flexibility and data sovereignty.[211]

Such policy tensions could hinder India's integration into the global AI innovation ecosystem and attract regulatory retaliation or digital trade friction with strategic partners.

4.5.5 Intellectual Property and AI-Generated Content

India's existing Copyright Act, 1957 and Patent Act, 1970 do not explicitly address whether AI can be considered an author or inventor. This leads to ambiguity in cases where AI autonomously generates content (e.g., art, music, code) or inventions (e.g., drug molecules designed by AI).

While Section 2(d)(vi) of the Copyright Act allows for non-human authorship in the case of computer-generated works, the term "person" in the statute implies human agency.[212] Similarly, patent law requires that inventors be natural persons, thereby excluding AI systems from being named as inventors.

This raises crucial legal questions: Should the developer, user, or owner of the AI system be credited? Can AI-generated outputs enjoy the same rights as human-created works? There is currently no judicial precedent or legislative guidance on these issues in India.

4.6 India in the Global Context

India's approach to regulating Artificial Intelligence (AI) and digital trade reflects a complex interplay of domestic priorities and international pressures. While India aspires to

[210] Digital Personal Data Protection Act, No. 22 of 2023, § 16(1), https://www.meity.gov.in/data-protection-framework.
[211] Ministry of Commerce and Industry, *India's Statement on WTO E-Commerce Negotiations*, (2020), https://commerce.gov.in. (Last visited Feb 2, 2025)
[212] Copyright Act, No. 14 of 1957, § 2(d)(vi) (India).

be a leader in digital innovation and AI adoption, it has adopted a cautious regulatory posture that emphasizes data sovereignty, strategic autonomy, and economic protectionism. In this context, it becomes critical to evaluate India's legal and policy stance in relation to global benchmarks. This section compares India's legal framework with that of major jurisdictions and multilateral negotiations to assess alignment, divergence, and future opportunities for convergence.

4.6.1 Comparative Overview: Global AI Regulatory Frameworks

European Union: The AI Act

The European Union's AI Act represents the world's first comprehensive legal framework for AI, based on a risk-based classification system. It mandates stricter compliance obligations for high-risk AI systems—such as those used in law enforcement, employment, or critical infrastructure—while banning systems that manipulate behaviour or engage in social scoring.[213]

Key features include:

- Mandatory conformity assessments for high-risk AI
- Transparency requirements for emotion recognition and biometric systems
- Explicit penalties for non-compliance (up to 6% of global annual turnover)

In contrast, India lacks a legislative framework that categorizes AI systems by risk or mandates ex ante assessments. Indian policy remains largely self-regulatory and fragmented across sectors, without any binding ethical or technical standards.

United States: Sectoral and Rights-Based Approach

The United States has taken a sector-specific and rights-based approach to AI governance, exemplified by its Blueprint for an AI Bill of Rights and recent Executive Orders.[214] This framework focuses on principles like:

- Algorithmic discrimination protection
- Data privacy and explain ability

---

[213] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206. (Last visited Mar 23, 2025)

[214] White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights* (Oct. 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

- Safe and effective AI use in healthcare, education, and employment

Although not legally binding, these principles are being operationalized through sectoral regulations and agency guidance. India's DPDP Act similarly enshrines consent and accountability principles but lacks dedicated mechanisms to prevent algorithmic discrimination or to provide a right to explanation.

China: AI Governance with Strong State Oversight

China has developed a stringent AI governance model characterized by centralized control, mandatory registration of AI algorithms, and strong surveillance-based applications. Regulations such as the Provisions on the Administration of Algorithmic Recommendations require companies to file algorithm details with regulators, enable users to opt out, and ensure ideological compliance.[215]

While India does not adopt ideological controls, its evolving policies on algorithmic accountability, non-personal data governance, and e-commerce regulation reflect a move toward sovereign regulatory control, albeit with democratic safeguards.

4.6.2 India's Digital Trade Policy in International Negotiations

India's stance on digital trade in multilateral forums has been marked by strategic protectionism. The country has opted out of several global initiatives due to concerns over regulatory autonomy, taxation rights, and cross-border data transfer obligations.

- WTO Joint Statement Initiative (JSI) on E-Commerce: India declined to join this plurilateral initiative, arguing that binding rules on data flows and source code disclosure could harm domestic industries and innovation.[216]
- Regional Comprehensive Economic Partnership (RCEP): India exited the RCEP partly due to concerns over digital trade provisions that might compromise local control over data.[217]
- Bilateral Free Trade Agreements (FTAs): India has negotiated data governance chapters in FTAs with the UAE, Australia, and the UK. These typically avoid

[215] Cyberspace Administration of China, *Provisions on the Administration of Algorithmic Recommendation in Internet Information Services* (Mar. 1, 2022), https://www.cac.gov.cn. (Last visited Mar 13, 2025)
[216] Ministry of Commerce and Industry, *India's Position on WTO E-Commerce Negotiations*, https://commerce.gov.in. (Last visited Mar 11, 2025)
[217] Press Information Bureau, *India's Withdrawal from RCEP Negotiations* (Nov. 2019), https://pib.gov.in.

binding commitments on unrestricted data flows, preferring broad, principles-based language.[218]

India's 2022 Draft National E-commerce Policy proposes data-sharing mandates for public interest and recommends that India retain the right to localize critical data. This signals India's preference for digital industrial policy over free-market liberalization in the digital space.

4.6.3 Convergence and Divergence with Global Norms

Dimension	**India**	**EU**	**U.S.**	**China**
Risk-based AI Regulation	No	Yes	No (sectoral)	Partial (classification under CAC)
Right to Explanation	No	Yes (GDPR Art. 22)	Guiding principle	No
AI Liability Laws	Underdeveloped	Draft AI Liability Directive	Product liability + agency actions	Vicarious & platform liability
Data Sovereignty	Strong emphasis	Liberal (with safeguards)	Liberal	State-controlled
Cross-Border Data Transfers	Conditional (trust-based)	Adequacy-based	Sectoral (FTC, HIPAA, etc.)	Severely restricted

[218] Department for Promotion of Industry and Internal Trade, *Draft National E-Commerce Policy* (Feb. 2019), https://dpiit.gov.in.

Algorithmic Transparency	Limited, sector-specific	Mandatory (for high-risk AI)	Recommended	Mandatory registration

India's position reflects a sovereignty-first digital governance philosophy. While it aligns with global norms in areas like data protection and intermediary liability, it diverges significantly in AI-specific regulation and digital trade liberalization.

4.6.4 Opportunities for Harmonization

Despite its divergences, India has significant opportunities to engage with global AI and digital trade governance:

- **Standard Setting**: India can participate in emerging ISO/IEC AI governance standards to shape global norms.
- **Data Transfer Protocols**: Creating a mutual adequacy regime with trusted trade partners can facilitate lawful AI development without compromising sovereignty.
- **Ethical AI Frameworks**: Adoption of non-binding but globally recognized ethical AI guidelines, such as those by OECD or UNESCO, may help India attract investment while maintaining public trust.
- **AI-Specific FTAs**: Future trade negotiations can incorporate safe harbour clauses, sandboxing provisions, and dispute resolution mechanisms tailored to AI-driven trade.

India’s regulatory pragmatism, if backed by institutional reforms, offers a path to responsible innovation, ensuring that AI and digital commerce flourish in a rights-respecting, globally interoperable framework.

4.7 Judicial and Legislative Trends

As Artificial Intelligence (AI) technologies gain traction in India, judicial and legislative developments have begun shaping the contours of AI governance and digital trade policy. Although courts have not yet directly adjudicated AI liability or algorithmic discrimination

cases, key constitutional judgments and parliamentary committee reports have laid foundational principles with long-term implications. This section surveys notable legal developments that inform the evolution of AI and digital trade regulation in India.

4.7.1 Judicial Engagement with Digital and Algorithmic Rights

India's judiciary has not explicitly ruled on AI regulation, but it has established legal doctrines highly relevant to algorithmic governance, particularly concerning privacy, data protection, and state surveillance.

Puttaswamy v. Union of India (2017)

In the landmark *Puttaswamy* case, the Supreme Court unanimously held that the **right to** privacy is a fundamental right under Article 21 of the Constitution, encompassing informational privacy, autonomy, and protection from state overreach.[219] The Court emphasized that data collection and processing must satisfy the tests of legality, necessity, and proportionality—principles central to regulating AI systems.

Although the case involved the Aadhaar biometric identification system, its reasoning applies equally to AI-based surveillance, profiling, and predictive analytics. The Court's stress on data minimization and purpose limitation provides a jurisprudential framework for challenging opaque AI systems.

Anuradha Bhasin v. Union of India (2020)

In another seminal decision, the Court recognized the internet as a medium essential for exercising fundamental rights and ruled that restrictions on internet access must be reasonable and proportionate.[220] This ruling has implications for AI-based content filtering, automated takedowns, and algorithmic censorship by intermediaries.

While Indian courts have not yet faced cases involving autonomous decision-making by AI, these precedents suggest that algorithmic opacity, bias, or arbitrariness in AI-based governance may be vulnerable to constitutional challenge.

4.7.2 Legislative and Regulatory Committee Reports

[219] *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India*, (2017) 10 S.C.C. 1 (India).
[220] *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637 (India).

Parliamentary committees have started recognizing the need to regulate algorithmic systems and digital markets. While their recommendations are not binding, they often serve as the basis for future legislation.

Standing Committee on Finance (2022): Big Tech and Market Competition

This report addressed anti-competitive practices by Big Tech platforms, including preferential ranking, self-preferencing, and lack of algorithmic transparency.[221] It called for the formulation of a Digital Competition Law and the establishment of a Digital Markets Unit within the Competition Commission of India to monitor and regulate algorithmic behaviour.

It recommended:

- Mandatory disclosures of algorithmic logic used in online marketplaces
- Audits of AI systems deployed by dominant platforms
- Algorithmic impact assessments for mergers and acquisitions

This marks a significant shift toward regulating AI-driven gatekeeping in digital commerce.

Committee on Information Technology (2021): Ethical AI

This committee explored the ethical dimensions of AI deployment and recommended:

- A National AI Ethics Framework
- Legal mandates for algorithmic explain ability and fairness
- A regulatory sandbox for AI innovation under MeitY[222]

While the report acknowledges India's digital ambitions, it urges caution against deploying AI without safeguards for rights, transparency, and accountability.

4.7.3 Draft and Proposed Legislative Developments

Digital India Act (Proposed)

In 2023, MeitY proposed the Digital India Act, intended to replace the IT Act, 2000. Though not yet introduced in Parliament, preliminary consultations suggest it will include:

- AI-specific definitions and classifications

[221] Parliamentary Standing Committee on Finance, *Report on Anti-Competitive Practices by Big Tech* (Dec. 2022), https://loksabhadocs.nic.in.

[222] Committee on Information Technology, *Ethical AI and the Future of Digital India*, Ministry of Electronics & IT (2021), https://meity.gov.in. (Last visited Apr 23, 2025)

- Guidelines on algorithmic accountability
- Clearer intermediary obligations for AI-generated content[223]

If enacted, it could become the first Indian law to directly regulate AI systems.

Personal Data Protection Bills (2019–2023)

Prior to the passage of the Digital Personal Data Protection Act, 2023, multiple iterations of data protection bills were debated, some of which proposed:

- Regulatory oversight over automated profiling
- User rights such as opt-out from AI processing
- Mandatory data audits for high-risk AI[224]

These proposals were diluted in the final Act, but they reflect a growing legislative intent to address AI-related privacy concerns.

4.7.4 Trends in Judicial Deference and Regulatory Gaps

While courts have laid the groundwork for rights-based AI governance, there is a noticeable judicial deference to executive policy in digital matters. For instance, judicial scrutiny of algorithmic content moderation by platforms has been limited, often framed as a private contractual issue rather than a public law concern.

At the same time, courts have urged the executive to create comprehensive digital laws, suggesting that judicial remedies alone are insufficient to regulate rapidly evolving AI ecosystems.

4.7.5 Outlook: Toward Proactive Legal Innovation

The convergence of judicial doctrine, legislative intent, and executive policy points to a transitional phase in India's AI legal framework. As AI technologies become more prevalent in public administration, financial systems, and consumer platforms, both ex ante regulations (pre-deployment assessments) and ex post remedies (legal accountability and redress mechanisms) will be essential.

India must institutionalize:

---

[223] Ministry of Electronics & IT, *Concept Note on the Digital India Act* (2023), https://www.meity.gov.in.
[224] Ministry of Law and Justice, *Personal Data Protection Bill (2019)* and Revised Drafts (2021), available at https://prsindia.org/billtrack.

- Algorithmic redress frameworks
- Regulatory bodies with AI-specific expertise
- Rights-based thresholds for AI deployment in sensitive domains

These measures will ensure that AI serves democratic objectives while minimizing systemic risks.

4.8 Challenges and Gaps in the Legal Framework

Despite India's growing digital economy and policy ambition to become a global leader in Artificial Intelligence (AI), its legal infrastructure remains fragmented, underdeveloped, and largely reactive. Several foundational and systemic gaps in India's legal framework inhibit the creation of a comprehensive, coherent, and future-ready AI and digital trade governance regime. This section identifies the most significant legal and institutional deficiencies.

4.8.1 Fragmentation of Regulatory Authority

One of the most pronounced challenges is the absence of a unified regulatory body for AI. Oversight is currently distributed across multiple agencies—such as MeitY, RBI, SEBI, TRAI, and proposed data protection authorities—without a centralized mechanism for coordination.[225]

This fragmentation leads to:

- Overlapping jurisdictions and inconsistent interpretations
- Delayed policy responses to rapidly evolving technologies
- Sectoral silos that hinder a holistic governance approach

For instance, both RBI and SEBI regulate AI-enabled financial platforms, yet there is no harmonized framework for algorithmic trading risk, consumer protection, or AI ethics.

4.8.2 Absence of AI-Specific Legislation

Unlike the European Union, which has drafted a comprehensive AI Act, India lacks any dedicated law or binding guidelines that define AI systems, categorize risk, or assign

[225] Ministry of Electronics & Information Technology, *Functions of MeitY*, https://www.meity.gov.in (last visited May 22, 2025).

responsibilities for transparency and accountability.[226]

Current laws:

- Do not distinguish between rule-based automation and machine learning-based AI
- Offer no ex-ante regulatory mechanism (e.g., AI system audits or risk classification)
- Provide no clear accountability structure for harms caused by AI

This legislative vacuum leaves critical questions—such as liability for autonomous decisions, requirements for fairness and explain ability, and safeguards for bias—unanswered in Indian law.

4.8.3 Inadequate Protection Against Algorithmic Discrimination

India's Digital Personal Data Protection Act, 2023, offers data privacy safeguards but does not prohibit algorithmic discrimination. Nor does it provide for a right to explanation, which would allow individuals to understand and contest AI-driven decisions impacting their rights and interests.[227]

This creates vulnerabilities in:

- Credit scoring and financial inclusion
- Employment screening
- AI-based public welfare delivery systems

The absence of mandated impact assessments, fairness audits, or algorithmic transparency standards undermines trust and exposes citizens to systemic harm.

4.8.4 Enforcement Asymmetry and Institutional Capacity Gaps

Even where legal provisions exist, enforcement capacity is uneven and under-resourced:

- Many regulators lack technical expertise to audit AI algorithms or assess bias
- Judiciary is yet to evolve AI-specific doctrines of liability, foreseeability, or negligence

---

[226] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final, https://eur-lex.europa.eu. (Last visited Dec 23, 2025)

[227] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India), https://www.meity.gov.in/data-protection-framework.

- Small and medium enterprises (SMEs) face disproportionate compliance burdens, while large tech platforms often operate in regulatory grey zones

The lack of institutional readiness can delay redressal, enable unchecked corporate practices, and erode public confidence in digital governance systems.[228]

4.8.5 Inconsistent Definitions and Terminologies

Key terms such as "AI system," "automated decision-making," "profiling," and "data fiduciary" are either undefined or inconsistently interpreted across statutes. This leads to:

- Ambiguity in obligations and scope of application
- Legal uncertainty for startups, developers, and multinational service providers
- Barriers to interoperability with global AI regulations and trade agreements

For example, the DPDP Act refers to "automated processing" but does not clarify its applicability to unsupervised learning or generative AI systems.

4.8.6 Limited Public Engagement and Transparency in Policymaking

Most AI-related policy drafts—including the National Strategy on AI, Draft E-Commerce Policy, and Non-Personal Data Governance Framework—have been prepared by executive committees without legislative debate or transparent consultation processes.[229] Civil society participation and technical expert engagement have often been limited to white papers, not binding law.

This top-down approach:

- Reduces democratic oversight
- Limits adaptability of law to diverse use cases
- Risks adoption of industry-favouring standards without sufficient public interest protections

4.8.7 Ambiguity Around Cross-Border AI Trade and Data Transfers

India's restrictive stance on data localization and its absence from global digital trade

[228] Centre for Internet and Society, *Comments on MeitY's Intermediary Guidelines*, https://cis-india.org (last visited May 22, 2025).
[229] NITI Aayog, *National Strategy for Artificial Intelligence – #AIforAll*, https://www.niti.gov.in. (Last visited Mar 23, 2025) (Last visited Jan 2, 2025)

platforms such as the WTO Joint Statement Initiative further complicate the legal environment for cross-border AI development.[230] While these policies are aimed at protecting digital sovereignty, they create:

- Uncertainty for foreign investors and cloud infrastructure providers
- Legal barriers to collaboration on global AI model training and deployment
- Potential trade conflicts under international law (e.g., Most Favored Nation treatment under GATS)

4.8.8 Ethical AI and Public Sector Deployment Risks

Several state-level and central government agencies are deploying AI tools in:

- Policing (facial recognition, predictive surveillance)
- Welfare delivery (automated beneficiary screening)
- Education (adaptive learning systems)

However, there are no legal mandates for ethical oversight, transparency disclosures, or bias assessments in these public applications, raising concerns about constitutional violations and lack of redress mechanisms for citizens adversely affected.[231]

4.9 Policy Recommendations and Reform Proposals

To ensure a responsible, competitive, and rights-based AI ecosystem, India must move beyond its current patchwork approach and institute a cohesive legal and policy architecture. This section outlines actionable reforms across legislative, regulatory, and institutional dimensions that aim to fill existing gaps, future-proof legal systems, and align India's digital governance with international best practices.

4.9.1 Enact a Comprehensive AI Regulation Framework

India should formulate a standalone Artificial Intelligence Regulation Act that:

- Defines AI systems and categorizes them by risk levels (e.g., minimal, limited, high, prohibited use)

[230] Ministry of Commerce and Industry, *India's Position on WTO E-Commerce Negotiations*, https://commerce.gov.in. (Last visited Jan 12, 2025)
[231] Internet Freedom Foundation, *Project Panoptic: Mapping Facial Recognition Technology in India*, https://panoptic.in. (Last visited Jan 21, 2025)

- Mandates pre-deployment audits for high-risk AI (e.g., in healthcare, policing, finance)
- Requires impact assessments to identify algorithmic harms and social implications
- Establishes penalties and civil liabilities for non-compliance

This approach can be modelled on the EU AI Act, while adapting it to India's democratic, socio-economic, and federal context.[232]

4.9.2 Establish a Central AI Regulatory Authority

To reduce fragmentation, India should constitute an independent National AI Governance Authority (NAGA) under MeitY or as a cross-sectoral body. NAGA's mandate should include:

- Licensing and registration of high-risk AI systems
- Oversight of AI deployments in public services
- Certification of algorithmic fairness and security standards
- Harmonization of sectoral guidelines (e.g., finance, telecom, education)

This institution should be empowered to coordinate with existing regulators (e.g., RBI, SEBI, TRAI) and provide a unified compliance ecosystem.[233]

4.9.3 Introduce Rights-Based AI Safeguards

India must enshrine a rights-based framework for AI governance through legislative amendments or secondary legislation under the DPDP Act, including:

- Right to explanation for automated decisions
- Right to opt-out of AI-based profiling
- Right to human oversight in high-impact decisions (e.g., healthcare denial, credit scoring)
- Mandatory algorithmic impact statements for public sector AI systems

These safeguards would strengthen compliance with Articles 14 and 21 of the Constitution, and align with the global trend toward ethical AI deployment.[234]

---

[232] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final, https://eur-lex.europa.eu.
[233] Ministry of Electronics & IT, *Concept Note on Digital India Act*, 2023, https://www.meity.gov.in.
[234] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).

4.9.4 Promote Ethical AI Through Public-Private Codes

Instead of heavy-handed regulation, India can promote industry-led ethical codes, backed by statutory oversight. These voluntary AI codes of conduct can cover:

- Fairness and non-discrimination
- Data governance practices
- Algorithmic transparency and accountability
- Redress mechanisms for affected users

Such frameworks, developed in partnership with industry, academia, and civil society, can foster regulatory innovation while ensuring accountability.[235]

4.9.5 Reform Intellectual Property Laws for AI Creativity

India should update its Copyright Act, 1957 and Patent Act, 1970 to address:

- Ownership of AI-generated works
- Attribution and licensing rights in collaborative human-AI creations
- Clarification of whether developers or users retain proprietary rights

Comparative jurisdictions such as the UK, Singapore, and Australia have begun legislative reviews in this area. India must balance incentives for innovation with equitable access and moral rights of human authorship.[236]

4.9.6 Align Digital Trade Policies with Global Frameworks

India must recalibrate its data localization and digital trade policies to:

- Establish mutual adequacy agreements for cross-border data flows
- Avoid isolation from global AI value chains
- Adopt interoperable standards for data transfer, cloud access, and algorithmic disclosures in trade pacts

Participation in plurilateral discussions (e.g., WTO JSI, IPEF digital chapters) should be reconsidered strategically, allowing room for policy flexibility without outright exit.[237]

---

[235] Internet Freedom Foundation, *Comments on AI Ethics and Accountability in India*, https://internetfreedom.in.
[236] Copyright Act, No. 14 of 1957, §§ 2(d)(vi), 13 (India); WIPO, *AI and IP Policy Report*, https://www.wipo.int/ai.
[237] Ministry of Commerce and Industry, *India's Digital Trade Policy Documents*, https://commerce.gov.in.

4.9.7 Strengthen Institutional Capacity and Judicial Expertise

- Invest in technical training for regulators and judges on AI technologies and forensic auditing
- Create AI law and policy cells in ministries and constitutional bodies (e.g., NHRC, CCI)
- Encourage publication of algorithmic impact reports and transparency benchmarks

This capacity-building approach ensures future-readiness and fosters proactive enforcement.[238]

4.9.8 Foster Innovation Through Sandboxing and Incentives

- Expand regulatory sandbox schemes for AI innovations beyond fintech (to include health tech, edtech, and logistics)
- Provide tax incentives and compliance credits for ethical AI developers
- Facilitate open data initiatives with anonymization protocols for public-interest AI research

These measures can enhance India's global **AI competitiveness** without compromising on ethics or legality.[239]

4.9.9 Embed AI Ethics in Public Sector Governance

AI systems used in public administration (e.g., predictive policing, biometric ID systems) should be subjected to:

- Independent audits and legislative oversight
- Public impact assessments and citizen consultation mechanisms
- Review by a public ombudsman or a digital rights tribunal

Embedding ethics in public AI use is key to maintaining public trust and legitimacy.[240]

---

[238] National Judicial Academy, *Training Module on Emerging Technologies and Law*, 2023, https://nja.gov.in. (Last visited April 30, 2025)
[239] Reserve Bank of India, *Regulatory Sandbox Framework*, https://rbi.org.in. (Last visited April 12, 2025)
[240] Internet Freedom Foundation, *Project Panoptic: Facial Recognition Audit Toolkit*, https://panoptic.in.

4.10 Conclusion

India stands at a critical juncture in the governance of Artificial Intelligence (AI) and digital trade. As the nation continues to advance its digital economy and embed AI across sectors—from finance and healthcare to education and governance—its legal and regulatory architecture must evolve accordingly. This chapter has demonstrated that while India has laid a foundational legal framework through instruments like the Information Technology Act,[241] Digital Personal Data Protection Act,[242] and e-commerce rules, these laws were not designed with AI's unique risks and complexities in mind. The fragmented institutional landscape, lack of AI-specific legislation, and insufficient safeguards against algorithmic discrimination and opacity highlight the pressing need for reform. Furthermore, India's cautious stance in global digital trade negotiations, while rooted in legitimate sovereignty concerns, risks isolating Indian innovation ecosystems from international collaboration and standardization.[243]

At the same time, judicial developments—particularly those affirming fundamental rights to privacy, equality, and transparency—offer a constitutional bedrock for shaping ethical and inclusive AI laws.[244] Legislative and parliamentary committee efforts indicate growing awareness of the challenges posed by unchecked AI proliferation, especially in relation to consumer protection, digital competition, and public accountability.[245]

To bridge the regulatory gap, this chapter proposed a comprehensive set of reforms including:

- A dedicated AI regulation framework based on risk classification and transparency obligations;[246]
- The creation of a central AI regulatory authority;

[241] Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India), https://www.meity.gov.in. (Last visited April 19, 2025)
[242] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India), https://www.meity.gov.in/data-protection-framework.
[243] Ministry of Commerce and Industry, *India's Position on WTO E-Commerce Negotiations*, https://commerce.gov.in. (Last visited April 12, 2025)
[244] Ministry of Commerce and Industry, *India's Position on WTO E-Commerce Negotiations*, https://commerce.gov.in. (Last visited April 12, 2025)
[245] Parliamentary Standing Committee on Finance, *Report on Anti-Competitive Practices by Big Tech* (Dec. 2022), https://loksabhadocs.nic.in.
[246] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final, https://eur-lex.europa.eu. (Last visited April 17, 2025)

- The incorporation of rights-based AI safeguards within data protection and public governance laws;[247]
- Revisions to IPR frameworks to accommodate AI-generated works;[248]
- Strategic alignment of cross-border digital trade norms**;**[249]

India must balance its regulatory aspirations with innovation incentives, ensuring that emerging legal regimes do not stifle ethical AI growth but rather channel it in ways that enhance democratic values, economic development, and international competitiveness. In sum, the future of AI and digital trade in India hinges not merely on technology adoption, but on the vision and coherence of the legal frameworks that govern it. A forward-looking, inclusive, and interoperable approach to AI regulation can secure India's place as a responsible global leader in the digital age.

[247] Ministry of Electronics & IT, Concept Note on the Digital India Act, 2023, https://www.meity.gov.in.
[248] Copyright Act, No. 14 of 1957; Patent Act, No. 39 of 1970 (India).
[249] Department for Promotion of Industry and Internal Trade, *Draft National E-Commerce Policy* (Feb. 2019), https://dpiit.gov.in. (Last visited April 16, 2025)

CHAPTER 5

CONCLUSION AND SUGGESTIONS

The intersection of Artificial Intelligence (AI) and international trade constitutes one of the most profound and far-reaching transformations of the 21st century. As AI technologies become embedded across the global trade ecosystem—optimizing supply chains, personalizing pricing models, automating dispute resolution, and driving platform-based commerce—the legal frameworks that govern these processes are facing an unprecedented challenge. This dissertation has aimed to provide a multidimensional legal and policy analysis of this technological convergence, with a special emphasis on India's evolving regulatory landscape within the broader international context.

At the heart of the analysis lies a critical observation: legal and institutional systems are consistently trailing behind the pace of technological innovation. The deployment of AI in trade processes has not merely augmented existing practices but fundamentally altered them, introducing unprecedented challenges. Traditional legal doctrines, rooted in human-centric models of liability, intent, and accountability, struggle to respond to the autonomous and opaque nature of AI-driven systems. Consequently, new legal questions have emerged—such as: Who is liable for errors made by self-learning algorithms? How can regulators ensure transparency in AI decisions that are based on non-linear, data-intensive models? What mechanisms exist to prevent discriminatory outcomes in AI-powered trade finance or customs clearance systems? These questions cannot be addressed adequately by the current frameworks, which were not designed to govern systems with such scale, speed, and complexity.

While various international organizations—such as the OECD, ISO, ITU, and the European Union—have developed voluntary standards and ethical guidelines for trustworthy AI, these efforts are often fragmented, non-binding, and lack enforcement mechanisms. The absence of a unified global regulatory regime has led to regulatory divergence, wherein countries pursue conflicting approaches—ranging from the EU's rights-based and risk-tiered regulatory approach to the U.S.'s sector-specific self-regulation

and China's centralized, state-centric oversight. Such disparities create legal uncertainty, increase compliance burdens for multinational enterprises, and may inadvertently erect new trade barriers in the digital economy.

From a trade law perspective, this regulatory fragmentation undermines core principles enshrined in instruments like the WTO's General Agreement on Tariffs and Trade (GATT) and General Agreement on Trade in Services (GATS), including non-discrimination, market access, and transparency. AI-based systems, if unregulated or poorly governed, can violate these principles through algorithmic bias, opaque trade decisions, and unequal access to automated services, leading to potential legal disputes and undermining trust in the multilateral trading system.

In India's case, the domestic legal infrastructure—though steadily evolving—remains predominantly reactive and sector-specific. Key statutes like the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, while foundational, lack specific provisions tailored to the unique risks and characteristics of AI. Regulatory authority remains dispersed among multiple bodies including MeitY, RBI, SEBI, TRAI, and sectoral ministries, with overlapping jurisdictions and limited coordination. Moreover, the absence of a dedicated AI law or a centralized regulatory authority has led to inconsistencies in policy implementation and weak enforcement of ethical standards.

However, India has taken notable steps forward, including the launch of the National Strategy on Artificial Intelligence by NITI Aayog, the development of regulatory sandboxes in the financial sector, and capacity-building initiatives under the Digital India framework. These efforts reflect a growing awareness of AI's transformative impact, yet they remain insufficient in the face of the systemic, cross-sectoral risks posed by AI in trade contexts.

To address these shortcomings, this dissertation proposes a set of integrated legal and policy reforms aimed at creating a coherent, forward-looking, and ethically grounded AI governance framework:

1. Unified Legal Framework: Establish comprehensive AI-specific legislation with clear definitions, scope, and jurisdictional clarity. The law should incorporate a risk-based classification system—similar to the EU's AI Act—that distinguishes between low-risk and high-risk AI applications and assigns appropriate obligations to each.
2. Algorithmic Transparency and Human Oversight: Mandate explain ability requirements, algorithmic impact assessments, and human-in-the-loop decision-making for all AI systems used in critical trade functions. These are essential for preserving due process and ensuring contestability of automated decisions.
3. Rights-Based Regulation: Enshrine digital rights in the AI regulatory framework, including the right to explanation, right to non-discrimination, and right to appeal AI-based decisions. These rights must be enforceable and supported by independent grievance redress mechanisms.
4. Institutional Capacity-Building: Invest in the training of regulators, judiciary, and legal professionals in AI technologies, data ethics, and algorithmic accountability. Specialized bodies—such as an AI Ethics Commission or a National AI Regulatory Authority—should be constituted to oversee implementation and enforcement.
5. Public–Private Partnership and Multistakeholder Governance: Foster structured collaboration between government agencies, industry leaders, academic researchers, and civil society to co-create governance frameworks, standards, and certification systems. Co-regulation and ethical co-design should become central to India's AI regulatory ethos.
6. International Engagement and Norm Alignment: India must take a proactive role in global AI governance, engaging with the WTO's Joint Statement Initiative on E-Commerce, participating in plurilateral digital trade agreements, and supporting the development of multilateral AI principles through platforms like the G20, OECD, and UNCTAD. Harmonizing domestic standards with international norms is essential for reducing trade frictions and fostering global trust in AI-enabled commerce.
7. Digital Sovereignty with Openness: India's approach must strike a balance between asserting digital sovereignty and ensuring openness to global innovation and data

flows. Protectionist measures—such as rigid data localization mandates—should not undermine the benefits of global AI collaboration or restrict the growth of cross-border digital trade.

Ultimately, this dissertation contributes to the broader academic and policy discourse that urges governments to move beyond reactive regulatory models and adopt anticipatory, ethical, and globally coordinated governance systems. It recognizes that AI regulation is not merely a technical exercise but a normative project that must be grounded in values of justice, equity, and democratic accountability.

The integration of AI into global trade is both an opportunity and a risk. It offers immense potential to accelerate economic development, streamline commerce, and foster innovation. Yet, if governed poorly, it can entrench existing inequalities, enable digital colonialism, and erode public trust. The law, therefore, must evolve not just to mitigate harm but to enable responsible innovation, uphold rights, and promote inclusive global prosperity.

In conclusion, the task before legislators, regulators, and global institutions is to construct an agile, inclusive, and principled governance architecture—one that ensures Artificial Intelligence serves as a tool for public good, rather than a vector of exclusion or inequality. As trade becomes increasingly algorithmic, the imperative is clear: we must regulate not just for the technologies of today, but for the futures we wish to create.

BIBLIOGRAPHY

BOOKS

1. KLAUS SCHWAB, *The Fourth Industrial Revolution* (World Econ. F. 2017).
2. ERIK BRYNJOLFSSON & ANDREW MCAFEE, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (W.W. Norton & Co. 2014).
3. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013).
4. CATHRINNE CATH, *Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges* (Royal Soc'y Rep. 2018).
5. CHRISTOPHER KUNER, *Transborder Data Flows and Data Privacy Law* (Oxford Univ. Press 2013).
6. VIRGINIA EUBANKS, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Press 2017).
7. PEDRO DOMINGOS, *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World* (Basic Books 2015).
8. DON TAPSCOTT & ALEX TAPSCOTT, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World* (Portfolio/Penguin 2016).
9. JOSEPH E. STIGLITZ, *Globalization and Its Discontents* (W.W. Norton & Co. 2002).
10. RAY KURZWEIL, *The Singularity is Near: When Humans Transcend Biology* (Viking 2005).

WORKS IN COLLECTION

1. Julie E. Cohen, *What Privacy Is For*, in Philosophical Dimensions of Privacy: An Anthology 85 (Ferdinand David Schoeman ed., 2019).

2. Daniel J. Solove, *A Taxonomy of Privacy*, in Readings in Cyberethics 427 (Richard A. Spinello & Herman T. Tavani eds., 2d ed. 2004).
3. Lawrence Lessig, *Code Is Law*, in The Future of Ideas: The Fate of the Commons in a Connected World 53 (Vintage Books 2002).
4. Luciano Floridi, *The Ethics of Artificial Intelligence*, in The Cambridge Handbook of Information and Computer Ethics 251 (Luciano Floridi ed., 2010).
5. Jack Balkin, *The Constitution in the National Surveillance State*, in The Constitution in 2020 203 (Jack M. Balkin & Reva B. Siegel eds., Oxford Univ. Press 2009).

ARTICLES

1. Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 *U.C. Davis L. Rev.* 399 (2018).
2. Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism, 20 *Theoretical Inquiries L.* 47 (2019).
3. Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information, 125 *Harv. L. Rev.* 1004 (2012).
4. Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 *Reg. & Governance* 505 (2018).
5. Danielle Keats Citron & Frank Pasquale, The Scored Society: Due Process for Automated Predictions, 89 *Wash. L. Rev.* 1 (2014).
6. Ugo Pagallo, The Laws of Robots: Regulating Autonomous AI, 31 *AI & Soc.* 537 (2016).
7. Ben Wagner, Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?, 13 *Law, Innovation & Tech.* 103 (2021).
8. Shoshana Zuboff, Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, 30 *J. Info. Tech.* 75 (2015).
9. Bryan Choi, The Fault in Software, 100 *Tex. L. Rev.* 105 (2021).
10. Mireille Hildebrandt, The Ethical Implications of AI in Legal Contexts, 33 *Law & Critique* 225 (2022).

INTERNET SOURCES

1. World Trade Organization, *How AI Shapes and Is Shaped by International Trade*, WTO News (Oct. 2023), https://www.wto.org/english/news_e/. (Last visited Jan 6, 2025)
2. United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2023*, UNCTAD (2023), https://unctad.org/.(Last visited Mar 12, 2025)
3. National Institute of Standards & Technology (NIST), *AI Risk Management Framework*, NIST, https://www.nist.gov/ (last visited April 14, 2025).
4. World Customs Organization (WCO), *AI in Customs Strategy and Data Processing*, WCO, https://www.wcoomd.org/ (Last visited Mar 28, 2025).
5. Organisation for Economic Co-operation and Development (OECD), *OECD Council Recommendation on Artificial Intelligence*, OECD/LEGAL/0449 (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (referenced in-text).(last visited Feb 15, 2025)
6. Indo-Pacific Economic Framework for Prosperity, *Digital Trade Pillar*, IPEF (2022), https://www.commerce.gov/ipef (inferred from citations and chapter references). (Last visited Jan 26, 2025).
7. G7, *Charter on Artificial Intelligence*, Hiroshima Declaration (2016), available at https://www.g7hiroshima2023.go.jp/ (accessed via in-text mention). (Last visited Apr 20, 2025).

REPORTS

1. Standing Comm. on Fin., *Report on Big Tech and Market Competition*, Lok Sabha Secretariat (2022).
2. Comm. on Info. Tech., *Report on Ethical AI*, Ministry of Elecs. & Info. Tech. (2021).

3. NITI Aayog, *Nat'l Strategy for Artificial Intelligence: #AIForAll*, Gov't of India (2018).
4. Ministry of Elecs. & Info. Tech., *Draft Nat'l E-Commerce Policy* (2022).
5. United Nations Conf. on Trade & Dev., *Digital Economy Report 2023* (2023).
6. Org. for Econ. Co-op. & Dev., *OECD Principles on Artificial Intelligence* (2019).
7. World Customs Org., *Guidelines on Artificial Intelligence in Customs* (2021).
8. Commission Proposal for a Regulation Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final (Apr. 21, 2021).
9. Fin. Action Task Force, *Opportunities and Challenges of New Technologies for AML/CTF* (2019).

WEBSITES

1. World Trade Organization, *How AI Shapes and Is Shaped by International Trade* (WTO News, Oct. 2023), https://www.wto.org/english/news_e/.(Last visited may 12, 2025)
2. United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2023* (2023), https://unctad.org/.(Last visited Apr 2, 2025)
3. National Institute of Standards & Technology (NIST), *AI Risk Management Framework*, https://www.nist.gov/ (accessed 2023). (Last visited Jan 14, 2025)
4. World Customs Organization (WCO), *AI in Customs Strategy and Data Processing*, https://www.wcoomd.org/.(Last visited April 1, 2025)
5. https://www.weforum.org/stories/2024/10/ai-global-trade-policymaking/
6. Elgar Hofmann & Matthias Rüsch, *Industry 4.0 and the Current Status as Well as Future Prospects on Logistics*, 89 COMPUT. IND. 23 (2017), https://doi.org/10.1016/j.compind.2017.04.002. (Last visited April 12, 2025)
7. Dmitry Ivanov & Alexandre Dolgui, *A Digital Supply Chain Twin for Managing the Disruption Risks and Resilience in the Era of Industry 4.0*, 142 TRANSP. RES. PART E: LOGISTICS & TRANSP. REV. 102190 (2020), https://doi.org/10.1016/j.tre.2020.102190. (Last visited Jan 12, 2025)
8. Ming Xu & Min Li, *Artificial Intelligence for Customs Inspection: A Review*, 166

EXPERT SYST. WITH APPLICATIONS 114061 (2021), (Last visited April 12, 2025)https://doi.org/10.1016/j.eswa.2020.114061. (Last visited Feb 12, 2025)

9. World Customs Org., *Study Report on Disruptive Technologies* (2020), https://www.wcoomd.org.
10. Ying Zhang & Yong Zhao, *Big Data Analytics for Cross-Border E-Commerce: Insights and Research Directions*, 38 ELEC. COM. RES. & APPLICATIONS 100897 (2019), https://doi.org/10.1016/j.elerap.2019.100897. (Last visited Jan 2, 2025)
11. Sadegh Saberi, Mohammad Kouhizadeh, Joseph Sarkis & Lejia Shen, *Blockchain Technology and Its Relationships to Sustainable Supply Chain Management*, 57 INT'L J. PROD. RES. 2117 (2019), https://doi.org/10.1080/00207543.2018.1533261.
12. Christopher Kuner et al., *International Regulation of AI: Issues and Directions*, 10 INT'L DATA PRIVACY L. 323 (2020), https://doi.org/10.1093/idpl/ipaa012.
13. Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter & Luciano Floridi, *The Ethics of Algorithms: Mapping the Debate*, 3 BIG DATA & SOC'Y 1 (2016), https://doi.org/10.1177/2053951716679679. (Last visited April 12, 2025)
14. Giovanni Sartor, *Artificial Intelligence and Legal Responsibility*, 378 PHIL. TRANSACTIONS ROYAL SOC'Y A 20190363 (2020), https://doi.org/10.1098/rsta.2019.0363. (Last visited Apr 3, 2025)
15. European Comm'n, *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust* (2020), https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.
16. Int'l Fin. Corp., Artificial Intelligence in Trade Finance: Current State and Future Outlook (2021), https://www.ifc.org. (Last visited Mar 23, 2025)
17. Sanae Ahmed & Andrei Zlate, *AI, Inequality, and Trade Finance Access in Developing Economies*, World Bank Pol'y Res. Working Paper No. 10108 (2022), https://documents.worldbank.org/en/publication/documents-reports/documentdetail/148321654530406662. (Last visited Jan 22, 2025)

18. European Comm'n, *Proposal for a Regulation on a European Approach for Artificial Intelligence (AI Act)*, COM (2021) 206 final (Apr. 21, 2021)..
19. Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, 22 COMPUTER L. REV. INT'L 97 (2021).
20. Office of Sci. & Tech. Pol'y, *Blueprint for an AI Bill of Rights* (2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
21. Elsa B. Kania, *China's AI Governance: Past, Present, and Future*, Ctr. for a New Am. Sec. (2020), https://www.cnas.org/publications/reports/chinas-ai-governance.
22. NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0) (2023), https://www.nist.gov/itl/ai-risk-management-framework.
23. FATF, Opportunities and Challenges of New Technologies for AML/CFT (2021), https://www.fatf-gafi.org.
24.]Hofmann, E. & Rüsch, M., Industry 4.0 and the Current Status as well as Future Prospects on Logistics, 89 Computers Ind. 23 (2017), https://doi.org/10.1016/j.compind.2017.04.002.
25. Ivanov, D. & Dolgui, A., A Digital Supply Chain Twin for Managing the Disruption Risks and Resilience in the Era of Industry 4.0, 142 Transp. Res. Part E 102190 (2020), https://doi.org/10.1016/j.tre.2020.102190.
26. Xu, M. & Li, M., Artificial Intelligence for Customs Inspection: A Review, 166 Expert Sys. with Apps. 114061 (2021), https://doi.org/10.1016/j.eswa.2020.114061.
27. World Customs Organization, Study Report on Disruptive Technologies (2020), https://www.wcoomd.org/.
28. Zhang, Y. & Zhao, Y., Big Data Analytics for Cross-Border E-Commerce: Insights and Research Directions, 38 Electron. Com. Res. & Apps. 100897 (2019), https://doi.org/10.1016/j.elerap.2019.100897.
29. Saberi, S., Kouhizadeh, M., Sarkis, J. & Shen, L., Blockchain Technology and Its Relationships to Sustainable Supply Chain Management, 57 Int'l J. Production Res. 2117 (2019), https://doi.org/10.1080/00207543.2018.1533261.
30. Kuner, C. et al., International Regulation of AI: Issues and Directions, 10 Int'l Data Privacy L. 323 (2020), https://doi.org/10.1093/idpl/ipaa012.

31. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S. & Floridi, L., The Ethics of Algorithms: Mapping the Debate, 3 Big Data & Soc'y (2016), https://doi.org/10.1177/2053951716679679.
32. OECD, Recommendation of the Council on Artificial Intelligence (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
33. Burrell, J., How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms, 3 Big Data & Soc'y 1 (2016), https://doi.org/10.1177/2053951715622512.
34. UNCTAD, Digital Economy Report 2021: Cross-border Data Flows and Development (2021), https://unctad.org/webflyer/digital-economy-report-2021.
35. WTO, Trade Facilitation Agreement Overview (2017), https://www.wto.org/
36. IEEE, P7003 - Algorithmic Bias Considerations Standard (2022), https://standards.ieee.org.
37. UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021), https://unesdoc.unesco.org/ark:/48223/pf0000381137.
38. United Nations, Roadmap for Digital Cooperation (2020), https://www.un.org/en/digital-cooperation-roadmap.
39. OECD, OECD Principles on Artificial Intelligence (2019), https://www.oecd.org/going-digital/ai/principles/.
40. Ivanov, D. & Dolgui, A., A Digital Supply Chain Twin for Managing the Disruption Risks and Resilience in the Era of Industry 4.0, 142 Transp. Res. Part E 102190 (2020), https://doi.org/10.1016/j.tre.2020.102190.
41. NIST, AI Risk Management Framework (2023), https://www.nist.gov/itl/ai-risk-management-framework.
42. UNCTAD, Digital Economy Report 2021: Cross-border Data Flows and Development (2021), https://unctad.org/webflyer/digital-economy-report-2021.
43. OECD, Recommendation of the Council on Artificial Intelligence (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
44. U.N. Dep't of Econ. & Soc. Affairs, *Sustainable Development Goals Report 2023*, https://unstats.un.org/sdgs/report/2023
45. G7 Hiroshima Leaders' Communiqué, G7 Summit (May 2023),

https://www.g7hiroshima.go.jp/documents/index.html.

46. See GDPR, Regulation (EU) 2016/679, arts. 22–23, 2016 O.J. (L 119) 1; cf. U.S. Nat'l Inst. of Standards & Tech. [NIST], *AI Risk Management Framework* (2023), https://www.nist.gov/itl/ai-risk-management-framework. (Last visited May 12, 2025)
47. World Trade Organization, *Work Programme on Electronic Commerce*, WT/L/274 (Sept. 1998), https://www.wto.org. (Last visited April 12, 2025)
48. NASSCOM, *AI Adoption in India: A Strategic Report*, 2023, https://nasscom.in.
49. Ministry of Electronics & Information Technology, *Digital India: Empowering Citizens*, https://www.digitalindia.gov.in. (Last visited April 2, 2025)
50. NITI Aayog, *National Strategy for Artificial Intelligence – #AIforAll* (2018), https://www.niti.gov.in/sites/default/files/2021-07/NationalStrategy-for-AI-Discussion-Paper.pdf. / Ministry of Health and Family Welfare, *Guidelines for Telemedicine in India* (2020) (Last visited Jan 2, 2025)
51. Reserve Bank of India, *Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps* (Nov. 2021), https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189. / Nasscom & BCG, *AI Adoption in Indian Enterprises* (2021), https://nasscom.in/knowledge-center/publications/ai-adoption-indian-enterprises.
52. Nasscom & BCG, *AI Adoption in Indian Enterprises* (2021), https://nasscom.in/knowledge-center/publications/ai-adoption-indian-enterprises. / Ministry of Electronics and Information Technology (MeitY), *Responsible AI for Social Empowerment (RAISE 2020) Summit Report*, https://www.meity.gov.in.
53. NITI Aayog, *National Strategy for Artificial Intelligence – #AIforAll* (2018), https://www.niti.gov.in/sites/default/files/2021-07/NationalStrategy-for-AI-Discussion-Paper.pdf. / Ministry of Agriculture and Farmers Welfare, *AI in Agriculture: Use Cases and Policy Suggestions*, Policy Brief No. 8 (2022), https://agricoop.nic.in. (Last visited April 12, 2025)
54. UNESCO, *AI and Education: Guidance for Policymakers* (2021), https://unesdoc.unesco.org/ark:/48223/pf0000376709. / NITI Aayog, *National Strategy for Artificial Intelligence – #AIforAll* (2018), (Last visited April 12,

2025)https://www.niti.gov.in/sites/default/files/2021-07/NationalStrategy-for-AI-Discussion-Paper.pdf. (Last visited April 12, 2025)

55. Internet Freedom Foundation, *Project Panoptic: Facial Recognition in India* (2021), https://panoptic.in. / Ministry of Electronics and Information Technology (MeitY), *Responsible AI for Social Empowerment (RAISE 2020) Summit Report*, https://www.meity.gov.in. (Last visited April 12, 2025)
56. Ministry of Commerce and Industry, *AI Task Force Report*, 2018, https://dpiit.gov.in. (Last visited April 12, 2025)
57. NITI Aayog, *National Strategy for Artificial Intelligence – #AIforAll*, 2018, https://www.niti.gov.in. (Last visited April 12, 2025)

STATUTES AND LEGAL INSTRUMENTS

1. Constitution of India (Jan. 26, 1950), arts. 14, 21.
2. Information Technology Act 2000, No. 21 of 2000, Acts of Parliament (India).
3. Digital Personal Data Protection Act 2023, No. __ of 2023, Acts of Parliament (India).
4. Consumer Protection Act 2019, No. 35 of 2019, Acts of Parliament (India).
5. Consumer Protection (E-Commerce) Rules, 2020 (India).
6. Copyright Act, 1957, No. 14 of 1957, Acts of Parliament (India).
7. Patents Act, 1970, No. 39 of 1970, Acts of Parliament (India).
8. Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154.
9. General Agreement on Tariffs and Trade, Marrakesh Apr. 15, 1994, 1868 U.N.T.S. 187.
10. General Agreement on Trade in Services, Marrakesh Apr. 15, 1994, 1869 U.N.T.S. 183.
11. Trade Facilitation Agreement, Dec. 8, 2013, WTO Doc. WT/L/940 (Mar. 31, 2016), 55 I.L.M. 316 (2016).
12. Information Technology Agreement, Dec. 5, 1996, 36 I.L.M. 354 (1997).

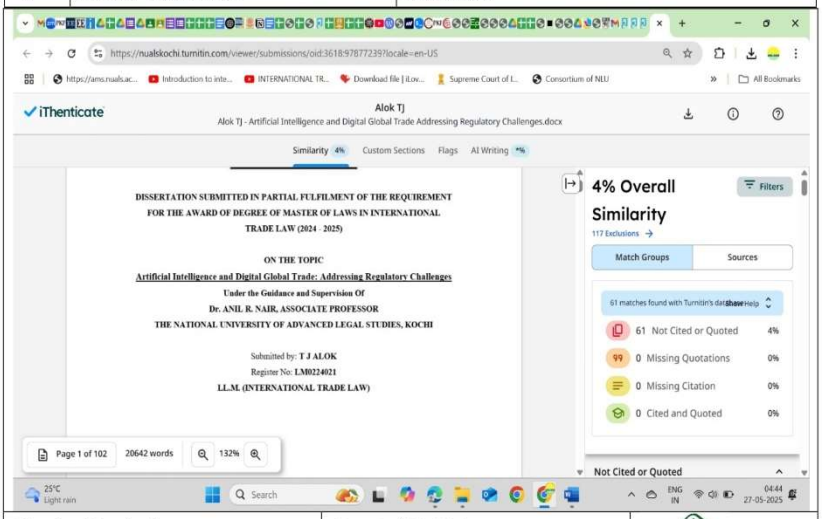
13. WTO Joint Statement on Electronic Commerce (2019).
14. Indo-Pacific Economic Framework for Prosperity – Digital Trade Pillar (2022).
15. OECD Council Recommendation on Artificial Intelligence (2019), OECD/LEGAL/0449.
16. G7 Charter on Artificial Intelligence (Hiroshima, 2016).
17. UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).
18. Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
19. Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act), COM(2021)206 final (Apr. 21, 2021).
20. ISO/IEC 23894:2023, *Information technology – Artificial intelligence – Risk management* (2023).
21. ISO/IEC TR 24028:2020, *Artificial intelligence – Overview of trustworthiness* (2020).
22. ISO/IEC 12792:202x (Draft), *Artificial intelligence – Bias in AI systems and datasets*.
23. ISO/IEC 38507:2022, *Information technology – Governance implications of the use of artificial intelligence* (2022).
24. NIST, *Artificial Intelligence Risk Management Framework* v1.0 (Jan. 26, 2023).
25. World Customs Organization, *AI in Customs: Ethical Guidelines and Strategy* (Dec. 2021).

APPENDIX

THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES
Kalamassery, Kochi – 683 503, Kerala, India

CERTIFICATE ON PLAGIARISM CHECK

1.	Name of the Candidate	Mr. T.J. Alok
2.	Title of Dissertation	Artificial Intelligence and Digital Global Trade: Addressing Regulatory Challenges
3.	Name of the supervisor	Dr. Anil R. Nair
4.	Similar content (%) identified	4%
5.	Acceptable maximum limit (%)	10%
6.	Software used	Turnitin
7.	Date of verification	27.05.2025



Checked By (with name, designation & signature)	Dr. Anil R. Nair, Associate Professor	
Name and Signature of the Candidate	Mr. T.J. Alok	
Name & Signature of the Supervisor	Dr. Anil R. Nair, Associate Professor	