Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Law and Emerging Technologies in Global Commerce: Regulatory Challenges in the Digital Transformation Era

Article History:

Name of Author:
Vedansh Sharma[1], Mr. Abhishek Kumar[2], Vidushi Verma[3], Shubham Prakash Singh[4], Dr. Kartik Agre[5]

Affiliation:
[1]Assistant Professor, School of Law, Faculty of Law, Manipal University, Jaipur
[2]Assistant Professor, TMCLLS, Teerthanker Mahaveer University, Moradabad
[3]Assistant Professor, School of Law, Galgotias University
[4]Assistant Professor, ICFAI Law School, ICFAI Foundation for Higher Education (deemed to be) University, Hyderabad.
[5]Assistant Professor (Senior Scale), School of Law, UPES, Dehradun.

Corresponding Author:
Vedansh Sharma

How to cite this article:
Sharma V, *et. al* Law and Emerging Technologies in Global Commerce: Regulatory Challenges in the Digital Transformation Era. *J Int Commer Law Technol.* 2025;6(1):549–554.

Received: *08-09-2025*
Revised: *22-09-2025*
Accepted: *05-10-2025*
Published: *23-10-2025*

Abstract: The article looks at how the rapid changing technological environments are critically intertwined with the legal and regulation frameworks which can change thereby affecting international trade. It examines the fact that the digital transformation, in particular, the role of technologies, including Artificial Intelligence and blockchain, is changing the foreign trade and modifying the existing legal framework with new risks. The introduction of the artificial intelligence into the field of global compliance in the trade, including, is expected to introduce a great deal of efficiency and classification accuracy into the specified sphere, though, it is also likely to introduce ambiguities as far as the specific definition and the implications the given sphere has on the stakeholders. Additionally, the extensive utilisation of fintech applications, including digital currencies and AI-based packages, weakens the traditional methods of transactions that are forced to re-examine the global consensus on trade and payment frameworks over the boundaries. The resulting cybersecurity challenges stemming from the growing number of threats to valuable information resources and critical infrastructure in this digital transformation have necessitated the need to redefine cybersecurity measures. It is equivalent to the legal issue related to smart weapons, cyber security and data protection and underscores the urgent need to collaborate globally and to establish robust global regimes to be in a position to address such issues. The fact that AI is currently extensively implemented in all these types of industries, namely healthcare, finance, transportation, etc., and the fact it is becoming a vital aspect of military, judicial, and international relations are multiplying these legal and ethical issues.

Keywords: Artificial Intelligence, International Trade Laws, Data Protection, Intellectual Property Rights, Trade Barriers, Regulatory Harmonisation

INTRODUCTION

The rapid appearance of digital technologies has changed the situation in the sphere of world trade, introducing a set of new legal and administrative concerns, which necessitates a paradigm shift in the existing systems. New technologies, such as artificial intelligence, blockchain, and the Internet of Things, add facilitation of this innovation and are not limited to the efficiencies of transactional aspects, but to some fundamental transformations in international trade, governance, and societal relations (Magableh, 2024). Despite the ease of global trade brought about by such technological integration, which is automated, and decision support is intelligent, it creates the concern of data security and normalization of laws across various jurisdictions (Khan, 2024). The proliferation of AI in the business world is something that needs a detailed consideration of how this will impact the legal frameworks that professed most jurisdictions,

particularly how the intellectual property rights will be legally safeguarded and whether or not trade remedies can be employed to address those effects. Besides that, the emergence of AI technologies mediate the given threats to the current regulatory frameworks through the introduction of new intricacies connected with such aspects as liability, bias in the algorithms, and the ethical guidelines of the autonomous systems in international trade (Liu, 2024). It will lead to a desire to develop adaptive legal systems that could react proactively to such problems rather than reactively to them through the implementation of reactive policies in order to implement anticipatory modelling and dynamic regulation approaches (Akpobome, 2024). Additionally, another radical possibility of efficiency and competitiveness lies in the introduction of AI in international trade agreements, yet it needs to be contemplated on the policy grounds to facilitate its implementation to the former systems (Igbinenikaro and Adewusi, 2024). The intricacy of the impact of digitalization to the global trade emphasizes even more the necessity of closing these regulatory gaps, especially because this phenomenon influences the competition of companies at the international level and determines the strategic location of states (Shlapak et al., 2023).

The Digital Transformation of Global Commerce

The system of digital trade is a dynamic one and to a significant extent, a volatile one, and the interaction of artificial intelligence and cybersecurity form a multi-dimensional and highly volatile situational environment that was quite profound at the global level and should be taken into careful and timely consideration. A mix of these conditions emphasizes a desperate necessity to form strong partnerships in other countries. This cooperation is necessary to design harmonized legal principles and adaptable regulatory frameworks that are capable of handling the complexity of digital business, reducing risks, and avoiding regulatory fragmentation, which at the same time can stimulate innovation and advance fair global growth (Khan, 2024). Nonetheless, the existing policy frameworks in use by nations are often limited in capability, as they often concentrate on physical infrastructure and adopt outdated definitions of cybersecurity threats, which are inadequate to contain the changing threat picture (Leal-Arcas et al., 2024). Such frameworks tend to fail to keep pace with the fast-changing technologies, which pose the danger of a regulatory loophole that the cybercriminals use to their benefit hindering the safe development of digital commerce (Gummadi, 2024). Systemic risks of the impact of the international system on national security, economic stability, and safety present themselves in the growing digitalization of trade and the growing use of AI within the international trade context due to the volume of data collection upon international networks, as well as the use of machine learning algorithms by offenders (Leal-Arcas et al., 2024). As such, a strategic balance between the national security interests and facilitation of free data flows across borders are required in order to govern the digital trade effectively (Zhang et al., 2024). This balancing exercise is additionally burdened with national approaches to data sovereignty that tend to place the firm, the state, or the individual in the forefront, thereby impeding cross-jurisdictional harmony and global functioning oneness (Zhang et al., 2024).

Challenges in Cross-Border Regulation

The diverse regulatory systems in the distinct jurisdictions specifically those of the regulation of data and electronic commerce are a notable obstacle towards the development of a consistent and reasonable global framework. This fragmentation is also compounded by the complex legal and regulatory issues that artificial intelligence technology poses to transnational data transfers, especially to data privacy protection, security and sovereignty.

Jurisdictional Complexities and Conflicts of Law

These complexities are usually due to varied requirements in countries in the form of legal frameworks that increase the cost of operation and legal risks to the enterprises involved in international trade (Chang, 2024). Besides, the difference in the regulatory approaches whereby certain countries focus more on the state-regulation of data whereas others focus on individual privacy or the autonomy of corporations poses a considerable difficulty of streamlining global digital trade policies (Zhang et al., 2024). This complicates the process of coming to an agreement on international norms to protect data and intellectual property, thus hindering the movement of goods and services across borders without any problems (Khan, 2024).

Harmonization vs. Fragmentation in International Law

The fact that the international regulations are being conflicting in a quest to implement international trade to ease international trade and the national legal systems have been actually divergent in their mainstreams poses a very valid challenge in creating a stable and predictable digital trade environment (Khan, 2024)(Chang, 2024). Such dichotomy is especially clear regarding artificial intelligence, as the national laws concerning data privacy and accountability tend to clash, making the creation and implementation of AI systems on the intercountry level difficult (Plinio, 2025). As an example, the

inconsistencies in the perception of data localization criteria and intellectual property rights associated with AI-generated content introduce serious obstacles to global cooperation and entry to the market (Israel, 2023)(SHARMA, 2024). This is further complicated by the fact that national interests are also differing as is the case between the market-based approach of the United States and the privacy-focused rules of the European Union that result in greater fragmentation in regulations (Minssen et al., 2025). To be more precise, the failure of multilateral organizations, such as the WTO, to transform in response to the changes to the digital trade has enhanced this fragmentation with states seeking unilateral or bilateral, or even regional agreements that further diverse legal frameworks to cross-border data flows (Chin and Jingwu, 2022).

Data Localization and Cross-Border Data Flows

The very existence of data localization requirements, frequently based on issues of national security or data sovereignty, hinders the actual cross-national movement of data directly, and thus erodes the efficiency and interdependency of digital trade on an international scale (Mishra and Kugler, 2024). The demands may cause higher operational expenses in enterprises, inhibit access to the international markets, and even suppress innovation through restrained data-driven insights (Mishra and Kugler, 2024). This is an especially acute problem in digital trade, where the lack of international data sharing regulations limits the use of new digital technologies across the national boundaries and prevents the trust in business, as the protection of intellectual property concerning digital algorithms remains weak at the same time (Cha et al., 2022). Therefore, having clear and coherent international data governance and intellectual property rights is of primary importance to ensure the alleviation of these issues and more integrated and functional global digital economy (Meltzer, 2019)(Osorio & Cruz, 2025).

Sector-Specific Regulatory Challenges

FinTech and Digital Payments

With the booming pace of FinTech, including blockchain-based payment engines and algorithmic trading, the agriculture of regulatory fear surrounding the stability, consumer protection, and anti-money laundering provisions of the financial stable system habitually lag behind the traditional financial regulation paradigm. This dynamism has brought about a competitive requirement of the ability to respond promptly to regulatory challenges that is available to the toleration of technological advancements and even to absorb systemic risks that these immature financial ecosystems may cause (AllahRakha, 2023). International FinTech platforms are allied to the growth of FinTech through often stiff legal rules, including data sovereignty risks, interoperability, and licensing (AllahRakha, 2023).

E-commerce and Consumer Protection

In addition, various national consumer protection laws, namely, in the field of data privacy and redress, are also an obstacle to cross-border operations and reduce the consumer confidence in international online shopping services (Minssen and Schovsbo, 2018). Another layer of complexity brought by differences in regulations in localities such as product safety, advertising regulations, and dispute resolution frameworks makes it challenging in regards to businesses complying with varying legal standards and customer redress (Joshi & Brahmbhatt, 2025). In the international expansion, regulatory obstacles to entering the e-commerce market are often related to the tax regimes and intellectual property, which demand adaptable strategies to enter the international market through legal measures (Ahi et al., 2022). In addition, international standards of consumer protection of digital products and services have not been uniform hence; it is hard to safeguard one against fraudulent activities and to offer equal treatment to the consumers across different jurisdictions.

Supply Chain Management and Traceability

Increased digitisation of supply chains through application of such technologies as IoT and blockchain are new challenges to establishing explicit legal accountability and data integrity within a globally distributed network of suppliers and logistics manufacturers. This would require attentive legal frameworks of intelligent contracts and data control to handle the mess of relationships and transactions within such complex systems. In addition to this, globalised contemporary supply chain and lack of a stable geopolitical environment represent other contributing factors of regulatory risk that appears in the form of compliance to sanctions and responsible sourcing requiring multi-layered and multi-faceted answers to the law. These problems are being compounded by the lack of legal provisions on the nature of supply chain information in cross-border level.

Ethical and Societal Implications

The huge impact of the new technologies on the society such as the way in which they can influence labor market and the level to which they may become commonplace in the course of spreading bias demands the ethical treatment when it comes to introducing regulations (Akpobome, 2024). This will require the regulators to abandon the purely economic dimension of compliance to the matters of equity, openness, and profitability in implementation and development of advanced technologies. Moreover, the dynamism with technology has often outpaced the legal provisions to create legal loopholes that may necessitate legal agility to predict

and address hitherto emergent challenges (Akpobome, 2024). These are preventative law practice paradigms such as the expropriation of technology solutions and professional counseling to enable law practices and remain abreast with the current dynamic regulations (Uwamusi, 2025). Protecting consumers by legal means and responsibilities is also more difficult, since the privacy and decentralization of some forms of digital payments, including cryptocurrency, complicates the task of tracing and implementing laws on consumer protection (Ballaji, 2024)(Zhuk, 2025). Such systems may be employed to perform illegal activities, which adds to this challenge and increases the necessity of implementing a strict regulation control (Ballell, 2019)(Szabo et al., 2024) further. Other than that, despite the fact that pseudonymous and decentralized blockchain technologies possess certain advantages, they are susceptible to data privacy and data safety vulnerabilities that, though may be partially addressed through the current legislation, need to be dealt with more efficiently than current legislation (Zhuk, 2025).

CONCLUSION

To overcome such weaknesses, there must be also a positive reinforcement of strong regulatory frameworks to strike the balance between innovation, and protect abuse and illicit affairs of financial services in the event of AI-based procedures that introduce new risks in the form of algorithm biasing and introduction of no transparency in automated decision-making (Mirishli, 2025)(SHARMA, 2024). This is especially relevant to such industries as financial markets, when the collapse of AI systems can cause a considerable impact on the safety of people and the stability of the market, in general (Montagnani et al., 2024). In this regard it becomes necessary that regulatory authorities adopt strong compliance framework, both in regard to explainability and data security, to address such risks efficiently (Mirishli, 2025). Additionally, the proper legal and regulatory frameworks of AI in the financial services sector should be designed to advance the objectives of market safety, consumer protection, and market integrity and fair access to finance (Lee, 2020). They should also take into account those ethical factors of AI as transparency, accountability, and fairness to eradicate such phenomena as discriminatory algorithms, which may be disproportionately applied to certain groups or lead to market manipulation (Uzougbo et al., 2024)(Sushkova and Minbaleev, 2021). The unceasing changes in the field of AI in the financial sector dictate new and continued adaptations to regulation, without which the transformational capacity of these technologies could be put into an irresponsible use and the stability of the system and trust in it as a whole would not be preserved (Alonso & Chatzianastasiou, 2024). It entails establishing more robust security measures in place of cyberattacks and data breaches and safeguarding intellectual property rights in the application of AI technologies(Uzougbo et al., 2024).

REFERENCE

1. Ahi, A., Sinkovics, N., & Sinkovics, R. R. (2022). E-commerce Policy and the Global Economy: A Path to More Inclusive Development? Management International Review, 63(1), 27. https://doi.org/10.1007/s11575-022-00490-1
2. Akpobome, O. (2024). The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation. International Journal of Research Publication and Reviews, 5(10), 5046. https://doi.org/10.55248/gengpi.5.1024.3012
3. AllahRakha, N. (2023). Legal Challenges for International Fintech Startups. International Journal of Law and Policy, 1(8). https://doi.org/10.59022/ijlp.148
4. Alonso, M. N. I., & Chatzianastasiou, F. S. (2024). The Case for Artificial Intelligence Regulation in the Financial Industry. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4831147
5. Ballaji, N. (2024). Consumer Protection in the Era of Digital Payments: Legal Challenges and Solutions. Beijing Law Review, 15(3), 1268. https://doi.org/10.4236/blr.2024.153076
6. Ballell, T. R. de las H. (2019). Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact. Uniform Law Review, 24(2), 302. https://doi.org/10.1093/ulr/unz018
7. Casalini, F., González, J. L., & Nemoto, T. (2021). Mapping commonalities in regulatory approaches to cross-border data transfers. OECD Trade Policy Working Papers. https://doi.org/10.1787/ca9f974e-en
8. Cha, H., Kotabe, M., & Wu, J. (2022). Reshaping Internationalization Strategy and Control for Global E-Commerce and Digital Transactions: A Hayekian Perspective. Management International Review, 63(1), 161. https://doi.org/10.1007/s11575-022-00494-x
9. Chang, Q. (2024). The Legal and Regulatory Issues of AI Technology in Cross-Border Data Flow in International Trade. Transactions on Economics Business and Management Research, 8, 111. https://doi.org/10.62051/cyw9y102
10. Chin, Y. C., & Jingwu, Z. (2022). Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. Laws, 11(4), 63. https://doi.org/10.3390/laws11040063

11. Gummadi, J. C. S. (2024). Cybersecurity in International Trade Agreements: A New Paradigm for Economic Diplomacy. American Journal of Trade and Policy, 11(1), 39. https://doi.org/10.18034/ajtp.v11i1.738
12. Igbinenikaro, E., & Adewusi, A. O. (2024). Policy recommendations for integrating artificial intelligence into global trade agreements. International Journal of Engineering Research Updates, 6(1). https://doi.org/10.53430/ijeru.2024.6.1.0022
13. Israel, D. (2023). Assessing the Effectiveness of Cross-Border Data Flow Regulations in the Age of Artificial Intelligence (AI). SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4448648
14. Joshi, S. M., & Brahmbhatt, G. (2025). Regulatory Challenges in Cross-Border Supply Chains. https://doi.org/10.2139/ssrn.5207622
15. Khan, A. (2024). THE INTERSECTION OF ARTIFICIAL INTELLIGENCE AND INTERNATIONAL TRADE LAWS: CHALLENGES AND OPPORTUNITIES. IIUM Law Journal, 32(1), 103. https://doi.org/10.31436/iiumlj.v32i1.912
16. Leal-Arcas, R., AlDamer, L., AlHokail, H., Saud, S. A. A., Alshaikh, S., AlSaud, S. F., Muhanna, S. A., Saud, L. F. A., Alaiban, N., & Alsaud, M. (2024). The Digitalization of Trade and Artificial Intelligence: a Pandora's box. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4816277
17. Lee, J. (2020). Access to Finance for Artificial Intelligence Regulation in the Financial Services Industry. European Business Organization Law Review, 21(4), 731. https://doi.org/10.1007/s40804-020-00200-0
18. Liu, J. (2024). Artificial Intelligence and International Law: The Impact of Emerging Technologies on the Global Legal System. Economics Law and Policy, 7(2). https://doi.org/10.22158/elp.v7n2p73
19. Magableh, N. Z. S. (2024). THE ADEQUACY OF THE LAWS REGULATING ELECTRONIC BUSINESS IN JORDAN. PUBLIC ADMINISTRATION AND LAW REVIEW, 66. https://doi.org/10.36690/2674-5216-2024-1-66
20. Meltzer, J. P. (2019). Governing Digital Trade. World Trade Review, 18. https://doi.org/10.1017/s1474745618000502
21. Minssen, T., & Schovsbo, J. (2018). Big Data in the Health and Life Sciences : What Are the Challenges for European Competition Law and Where Can They Be Found? Research Portal Denmark, 5, 121. https://local.forskningsportal.dk/local/dki-cgi/ws/cris-link?src=ku&id=ku-d8afafed-a889-4288-a219-516dd710c8c7&ti=Big%20Data%20in%20the%20Health%20and%20Life%20Sciences%20%3A%20What%20Are%20the%20Challenges%20for%20European%20Competition%20Law%20and%20Where%20Can%20They%20Be%20Found%3F
22. Minssen, T., Smith, H. J., Mann, S. P., García, A. M., & Negrete, J. (2025). THE EUROPEAN AI ACT : PROMISES, PERILS & TRADE-OFFS IN A COMPLEX REGULATORY ECOSYSTEM. Research Portal Denmark, 1, 330. https://local.forskningsportal.dk/local/dki-cgi/ws/cris-link?src=ku&id=ku-2fbecc26-4adb-487a-92d7-469ae5a7b774&ti=THE%20EUROPEAN%20AI%20ACT%20%3A%20PROMISES%2C%20PERILS%20%26amp%3B%20TRADE-OFFS%20IN%20A%20COMPLEX%20REGULATORY%20ECOSYSTEM
23. Mirishli, S. (2025). Regulating Ai In Financial Services: Legal Frameworks And Compliance Challenges. arXiv. https://doi.org/10.48550/ARXIV.2503.14541
24. Mishra, N., & Kugler, K. (2024). INTERNATIONAL COMMUNITY IN THE GLOBAL DIGITAL ECONOMY: A CASE STUDY ON THE AFRICAN DIGITAL TRADE FRAMEWORK. International and Comparative Law Quarterly, 1. https://doi.org/10.1017/s0020589324000290
25. Montagnani, M. L., Najjar, M.-C., & Davola, A. (2024). The EU Regulatory approach(es) to AI liability, and its Application to the financial services market. Computer Law & Security Review, 53, 105984. https://doi.org/10.1016/j.clsr.2024.105984
26. Osorio, C. P., & Cruz, J. (2025). Promoting free flows via competition law: An AI industry blueprint for Southeast Asia. Telecommunications Policy, 102953. https://doi.org/10.1016/j.telpol.2025.102953
27. Plinio, S. D. (2025). Panta Rh-AI: Assessing multifaceted AI threats on human agency and identity. Social Sciences & Humanities Open, 11, 101434. https://doi.org/10.1016/j.ssaho.2025.101434
28. SHARMA, DR. N. (2024). ARTIFICIAL INTELLIGENCE: LEGAL IMPLICATIONS AND CHALLENGES. Knowledgeable Research A Multidisciplinary Journal, 2(11), 13. https://doi.org/10.57067/220k4298
29. Szabó, J., Bernard, C., & Philip, L. T. (2024). Legal Implications and Challenges of Blockchain Technology and Smart Contracts. Jisuanji

Shenghuojia., 12(2), 6. https://doi.org/10.54097/ztn2w848

30. Uwamusi, J. A. (2025). Navigating complex regulatory frameworks to optimize legal structures while minimizing tax liabilities and operational risks for startups. International Journal of Research Publication and Reviews, 6(2), 845. https://doi.org/10.55248/gengpi.6.0225.0736
31. Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). Legal accountability and ethical considerations of AI in financial services. GSC Advanced Research and Reviews, 19(2), 130. https://doi.org/10.30574/gscarr.2024.19.2.0171
32. Zhang, C., Chen, X., Yang, J., & Gao, X. (2024). Nexus between digital trade and security: geopolitical implications for global economy in the digital age. Asian Review of Political Economy, 3(1). https://doi.org/10.1007/s44216-024-00032-6
33. Zhuk, A. (2025). Beyond the blockchain hype: addressing legal and regulatory challenges. SN Social Sciences, 5(2). https://doi.org/10.1007/s43545-024-01044-y
34. Сушкова, О. В., & Minbaleev, A. (2021). Legal regulation of artificial intelligence in the financial services market: a comparative analysis. SHS Web of Conferences, 118, 4007. https://doi.org/10.1051/shsconf/202111804007
35. Шлапак, А., Yatsenko, О., Іващенко, О. А., Zarytska, N., & Osadchuk, V. (2023). DIGITAL TRANSFORMATION OF INTERNATIONAL TRADE IN THE CONTEXT OF GLOBAL COMPETITION: TECHNOLOGICAL INNOVATIONS AND INVESTMENT PRIORITIES. Financial and Credit Activity Problems of Theory and Practice, 6(53), 334. https://doi.org/10.55643/fcaptp.6.53.2023.4241

