ORIGINAL RESEARCH PAPER
Volume - 14 | Issue - 06 | June - 2025 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

AI REGULATION IN CROSS-BORDER E-COMMERCE: LEGAL CHALLENGES AND GLOBAL REMEDIES

Management

Omolsalameh Pakuhinezhad University of Kerala. India.

Nastaran Afsham Faculty of Entrepreneurship, University of Tehran, Tehran, Iran.

ABSTRACT

Cross-border e-commerce is being remodeled through the application of artificial intelligence (AI), yet this is also creating extensive legal problems. The article elaborates on the intricate issues of the governance of AI across different jurisdictions with a focus on the foremost legal challenges of jurisdictional authority, data security, intellectual property rights, algorithmic bias, and liability. The divergence of regulatory regimes in major jurisdictions the European Union, United States, and China creates fragmentation that disrupts global operations and undermines consumer confidence. Through comparative analysis, the paper discerns the weaknesses and strengths of these regulatory frameworks and urges immediate international cooperation on the formulation of consistent, transparent, and stable AI governance. The paper advocates for clear legal obligations on AI accountability, algorithmic transparency, and digital rights protection, with the aim of obtaining a regulatory framework that is able to drive innovation while safeguarding consumer rights and promoting fairness in the digital economy. Lastly, the paper calls for international harmonized efforts to mitigate the risks of AI in cross-border e-commerce while its potential is fully exploited.

KEYWORDS

AI Regulation, Cross-Border E-Commerce, Legal Harmonization, Algorithmic Transparency, Jurisdictional Conflict

INTRODUCTION

The rapid advancement of AI-driven technologies, particularly in fields like robotics and education, has positioned AI as a cornerstone of the digital economy. Cross-border e-commerce exemplifies this transformation, leveraging AI innovations such as personalized customer insights and automated logistics to redefine global trade [1,33].From personalized recommendations to pricing algorithmics, from AI-powered logistics to automated customer service, these technologies are revolutionizing international commerce, releasing unprecedented efficiency and scalability [2]. Yet, as more and more global transactions are mediated by AI systems, their regulation has been a priority legal challenge. The global nature of e-commerce clashes with territorially anchored systems of national laws, creating a thicket of jurisdictional conflicts, data sovereignty issues, and unresolved ethical challenges [12, 19]. Unlike traditional trade regulations, which operate within well-defined boundaries, AI's pervasive and adaptive nature defies conventional legal categorizations, leaving gaps in accountability, transparency, and consumer protection [4, 7, 13]. This tension is fueled by the varying regulatory philosophies of world economic leaders: a strongly regulated, rights-based approach from the European Union [2, 8, 9]; market-friendly pragmatism from the United States [, 27, 34]; and a state-led model from China [5, 18, 35], each trying to shape the worldwide AI regulatory paradigm in forms that are consonant with their economic and political interests.

The price for this regulatory fragmentation is steep. Consider the case of algorithmic bias: an AI-based recruitment program of a multinational corporation discriminates against one demographic group of hires, but litigation gets muddled when the software was developed in one jurisdiction and tested using data from another, then deployed in a third [17]. Similarly, when a self-delivery drone causes property damage across national borders, liability codes—long written for human actors or stationary goods—don't easily assign blame to developers, operators, or even the AI itself [14]. Compounding these are the enormous data flows backing AI systems, which conflict with incompatibly differing national regimes like the EU's General Data Protection Regulation (GDPR), which insists on robust user consent and localization of data [9], and China's Cybersecurity Law, which prioritizes state surveillance over individual privacy [19]. The absence of harmonized standards forces businesses into costly compliance somersaults, wherein compliance with one set of rules can be incompatible with another's, and can chill innovation and erode consumer trust in cross-border digital marketplaces [11, 12].

This patchwork of regulation undermines even the potential of AI for international e-commerce. For instance, while AI can streamline customs clearance and reduce fraud, disparate regulations on algorithmic transparency—e.g., the EU's "explainability" mandate for high-risk AI systems versus the U.S.'s reliance on post hoc audits—leave developers and users in limbo [8, 36]. Intellectual property rights merely complicate matters further: if an AI creates a patented invention or copyrighted material, powers do not agree on whether it is the programmer's, end-user, or nobody's [28]. Such open questions deter investment and cooperation, particularly for small and medium-sized businesses with no resources to resolve such complexity. While so, the lack of international frameworks for international liability leaves AI-generated harm victims—whether discriminatory credit scoring or failed autonomous systems—without meaningful recourse, further exacerbating inequality in the digital economy [37]. In such a context, the need for international coordination becomes overwhelming. The EU's proposed AI Act and the OECD's AI Principles set out nascent templates for risk-based regulation [8, 23], but they will succeed only through global-scale uptake and enforcement symmetry [21, 24]. Trade agreements like the WTO's e-commerce negotiations might include AI-specific provisions placing data flows and responsibility in code [32], and intergovernmental organizations like the UN Advisory Group on AI have to weigh ethical considerations against commercial interests [29]. Ultimately, whatever mechanism is being harmonized will have to strike a balance between incentivizing innovation and protecting against the societal risks of AI so that fairness, transparency, and accountability are not lost to competitive pressure [7, 15]. This argument holds that the future lies not in unilateral hegemony—whether the "Brussels Effect" [2, 26] or techno-authoritarian forms [18]—but in collective governance that reconciles legal certainty with ethical imperatives. By examining the interplay of jurisdictional conflicts, comparative regulatory strategies, and emergent solutions, this study seeks to chart a course toward a cohesive global regime—one that harnesses AI's potential for cross-border commerce while mitigating its threats to fundamental rights and market integrity.

The Legal Issues of Regulating AI

Regulatory complexity of artificial intelligence in cross-border e-commerce is formidable and costly. The legal framework is constantly evolving, driven by technological progress and the forces of global markets [6]. The following are the most critical legal concerns that arise when regulating AI in cross-border commerce:

Table1: Core Legal Challenges In Regulating AI In E-commerce

Legal Issue	Description	Cross-Border Impact
Jurisdiction	Determining applicable laws and courts	Legal fragmentation across borders
Data Protection	Managing personal data across nations	Conflicting standards and enforcement gaps
Intellectual Property	Ownership of AI-generated content	Inconsistent IP protection
Algorithmic Bias	Discriminatory results from biased training data	Amplifies global inequality
Liability	Assigning responsibility for AI-caused harm	Lack of international liability frameworks

A. Jurisdiction And Enforcement

One of the most salient legal concerns for cross-border regulation of AI is determining the right jurisdiction for legal standard enforcement. AI systems operate across different jurisdictions, and it is difficult to determine under whose jurisdiction conflicts relating to AI technologies ought to be decided [12].

Conflicting National Norms:
Each country has different norms for handling AI, resulting in possible conflicts. For example, in the EU, stringent rules are kept by the GDPR for personal data usage [9], whereas the United States has more patchy legislation on data protection [34]. This results in a patchwork of laws in terms of applicability, which becomes confusing for multinationals with international operations [12].

Enforcement Mechanisms:
Enforcement of AI regulations can be particularly challenging where the responsible body is outside one's jurisdiction. Businesses can sometimes have more than one jurisdiction of operation, and there might not be an effective method of coordinating enforcement across different jurisdictions. This provides a loophole in legal liability where businesses may exploit regulatory loopholes [13].

Jurisdictional Uncertainty Of Cross-border Transactions:
Cross-border e-commerce generally entails data transmission across jurisdictions. However, not all jurisdictions have clear and enforceable rules on data protection, liability of artificial intelligence, and dispute resolution. Such uncertainty undermines the effectiveness of AI regulation and enhances the consequences of non-compliance, especially for multinational businesses that operate in multiple jurisdictions [11].

B. Data Protection and Privacy
With AI relying on information for its operations, data protection is one of the most important issues in AI regulation. The storage, collection, and processing of individual data raises significant privacy concerns, especially when data are involved across borders. AI models would require large quantities of data that cross multiple jurisdictions, and thus it is difficult for regulators to protect consumer privacy [19]. In the EU, there is the GDPR that has stringent data processing and data subject rights regulations [9], but most nations do not have similar strictures. It is difficult for companies to apply multiple, conflicting data protection regulations [11].

C. Intellectual Property (IP) Rights
AI raises many questions about intellectual property rights, especially for AI-generated work. Traditional IP models were developed for human writers and can, in theory, be lacking when taking into account the sophistication of AI innovation [28].

1. Ownership of AI-Generated Work: AI computers are capable of generating original content, i.e., music, paintings, inventions. The question arises of who owns the rights to the resulting work of art. In the majority of legal frameworks, copyright law is unclear on whether a work produced by AI can be copyrighted and who should be entitled to be considered as the author. For example, if an artificial intelligence invents something new, should intellectual property rights be granted to the AI inventor, the user of the AI, or the AI itself? [28]

2. Patentability of AI Inventions: Patent laws are also a source of concern. Whether or not inventions made by artificial intelligence can be patented and who has the patent rights is a matter of dispute. Various nations have different approaches to this problem, with some permitting patents based on AI-created inventions and others refusing to do so [28].

3. Global IP Harmonization: The differential levels of protection of IP across countries also render regulation of AI challenging. Harmonization of global IP laws is necessary to guarantee that companies may travel unimpeded across the globe, especially when the innovation in question is AI-based [28].

4. Consumer Consent and Transparency: One of the underpinning principles of data protection is that consumers must give informed consent if they wish their personal data to be processed. However, the non-transparency of AI systems—particularly where the data which they process and how it becomes processed is concealed—makes it difficult for consumers to know what they are consenting to. Non-transparency erodes consumer trust and makes the success of consent-based data protection regimes less effective [4].

5. Cross-Border Data Transfers and Regulation Gaps: The transfer of data across borders is the most important problem with AI regulation when there is personal data involved. Jurisdictions like the EU have attempted to deal with it using arrangements such as the Privacy Shield and Standard Contractual Clauses [9], but little is uniform when it comes to the way various states deal with cross-border data transfers. Such fragmentation makes the global implementation of data protection controls contentious [11, 19].

D. Algorithmic Bias and Ethical Issues
Algorithmic bias is likely the biggest ethics problem with AI systems. Training algorithms from previous data are also able to mirror and even amplify existing bias in society. These biases have the potential for resulting in discriminatory outcomes in fields from employment to credit to law enforcement [17].

Effect on Marginalized Communities:
AI technologies, no matter how well conceived, may end up having a worse effect on marginalized communities. Predictive policing algorithms, for example, may have a disproportionately negative effect on minority communities, and recruitment algorithms may operate disproportionately for certain groups [17]. These raise significant concerns about the fairness and equality of using AI technologies.

1. Insufficient Accountability for Bias Results: Several AI tools work as "black boxes" under which decision-making processes remain hard to follow. It makes them hard to blame developers and firms for causing unfair or prejudicial results. Regulation standards, calling for focus on transparency and accountability of algorithms, are required in order to fight these problems [4].

2. Ethical Design of AI: AI technologies must be designed ethically to avoid discrimination. This requires that ethical principles and standards are applied in a bid to ensure fairness, transparency, and inclusion when designing and using AI technologies [7, 15].

E. Liability And Accountability
As autonomous AI systems become increasingly common, it is increasingly hard to assign liability for harm caused by AI technologies. AI technologies have the capability of making decisions with far-reaching consequences, but accountability for such decisions is generally vague [14].

1. Product Liability and Artificial Intelligence: The traditional product liability laws, which place liability on manufacturers for faulty products, have no application to accidents and injuries resulting from AI. For example, with driverless cars employing artificial intelligence, no one knows who is to be blamed in the event of an accident, the manufacturer, the software developer, or the user.

2. Liability for Algorithmic Choices: If AI systems make choices—credit scoring or employment, for instance—who makes the decision? If AI systems harm individuals, how does one determine liability? This is an important question that needs to be answered through coherent and consistent legal frameworks [14].

II. Comparative Legal Approaches To AI Regulation
In a bid to effectively address the challenges of AI regulation in cross-border e-commerce, there is a need to study the regulatory approaches employed by different jurisdictions. Herein, this paper discusses how the European Union, the United States, and China regulate AI and the consequences of the different frameworks. "The EU, U.S, and China have adopted divergent regulatory strategies in response to these challenges" [6, 12].

Table 2: Comparative Overview Of AI Regulatory Approaches

Feature	European Union	United States	China
Data Protection Law	GDPR	CCPA (California); Fragmented	Relatively weak, surveillance-heavy
AI-Specific Legislation	Draft AI Act	No federal AI law	Multiple policies; vague
Enforcement Mechanism	Centralized	Sector-based, state-driven	State-controlled

Transparency Requirements	High	Moderate	Low
Accountability Requirements	Emphasized	Ambiguous	Varies
Criticism	Complex compliance	Lack of uniformity	Privacy and rights concerns

(Note: The table is referenced but not included in the original text, so no citations are added for it.)

A. The European Union (EU)

The EU is a global leader in artificial intelligence regulation, thanks in part to the implementation of the General Data Protection Regulation (GDPR) and the forthcoming Artificial Intelligence Act [2, 8, 9].

1. GDPR and Consumer Protection: The European Union's regulatory approach is aimed at consumer protection rights, transparency, and accountability. It oversees how companies collect, hold, and process personal data, and it has strict sanctions for artificial intelligence systems grounded on it. The General Data Protection Regulation's focus on consumer consent and protecting data has established a global benchmark for privacy law [9].

2. The Artificial Intelligence Act: The European Union bill aims at placing regulation on high-risk artificial intelligence systems such as those used in the health sector, transportation, and law enforcement. The AI Act suggests a risk-based approach to regulation that requires companies to demonstrate their AI systems are transparent, fair, and accountable [8].

3. Implementation Issues: Even though the EU's regulatory model is integrated, its implementation is an issue. Businesses operating in the EU have to deal with complex compliance processes, and international cooperation in implementing the AI Act in a global context is a topic of discussion [2, 13].

4. Building Accountability in Global E-Commerce: In international e-commerce, frameworks need to be established to hold companies accountable when AI systems cause harm to consumers. These frameworks need to allow for the imposition of sanctions for breach of AI rules and for enforcement of consumer protection laws [8].

B. The United States

In contrast to the EU's top-down approach, the United States has used a more market-driven and decentralized approach to regulating AI. Federal regulation of AI is still in its beginning stages, with various agencies adopting varying approaches to regulating AI [1, 27].

1. Federal Trade Commission (FTC) Regulation: The FTC regulates AI technologies primarily within the realm of consumer protection and antitrust. Industry guidelines have been issued by the FTC to advise companies that the AI systems need not be deceptive and not unfair to consumers [1].

2. Sector-Specific Regulations: In the absence of comprehensive federal regulation, individual states have been enacting their own regulations on AI and data privacy. California's Consumer Privacy Act (CCPA), for example, has required robust data privacy regulations for businesses operating within the state [34].

3. Problems of Harmonization: The U.S. has no single, national regulatory scheme, which hinders businesses that operate across states. The devolved system can make it impossible to have one global standard in AI regulation [6, 34].

C. China

China opted for a more centralized regulation mode of AI, where the government occupied the front-line role of driving AI innovation and AI application regulation [5, 18].

1. AI Development Strategy: China's AI development strategy is articulated through two government objectives: becoming the world leader in AI by 2030 and creating China as an AI superpower. The government has initiated many policies favoring AI innovation, such as backing AI start-ups and research centers [5, 35].

2. Privacy and Security Concerns: Criticism of China's AI policy has also been that it does not sufficiently address privacy and human rights concerns. The government's eagerness for surveillance technologies and data collection has raised civil liberties concerns and the risk of artificial intelligence systems manipulating society [18, 38].

3. Regulatory Uncertainty: While several regulations have been established by China regarding AI, the laws typically are unclear in nature and open to interpretation. The legal framework must be more transparent so that businesses as well as consumers could rely on known and predictable patterns of rules [18].

III. Proposed Solutions to Harmonize AI Regulation

Considering the above challenges and regulatory fragmentation, this paper proposes several solutions to harmonize AI regulation across the globe.

A. International Cooperation and Standardization

With the worldwide applicability of AI technologies, cooperation at the global level is essential to develop aligned and consistent regulatory strategies. International organizations such as the World Trade Organization (WTO), the Organization for Economic Co-operation and Development (OECD), and the International Telecommunication Union (ITU) can facilitate discussion between governments and develop global standards for regulating AI [21, 23, 24, 32].

B. Algorithmic Transparency and Accountability

To build public trust in AI, there is a need for regulatory requirements of algorithmic transparency. Governments must ensure it becomes mandatory for AI developers to disclose the steps taken in algorithms, provide explanations of automatic decisions, and create provisions for being held accountable when AI systems result in harm [4, 16].

C. Somewhat More Transparent Data Protection and Consumer Safeguards Legislation

A harmonized approach to data protection and consumer protection must be implemented in order to facilitate cross-border e-commerce. A global framework based on the principles of the GDPR would be capable of harmonizing data protection law and ensuring that consumer rights are upheld across borders [9, 11].

D. Developing Global Liability and Accountability Frameworks

In order to address the legal ambiguity of liability in harm caused by AI, there ought to be an international framework for liability. This framework should demarcate clear lines of liability for firms and individuals using AI systems, particularly when such systems are dangerous for consumers or encroach on law rights [14, 38].

CONCLUSION

The rapid expansion of artificial intelligence (AI) in cross-border e-commerce has both vast possibilities and grave challenges. The worldwide nature of AI technologies, along with the complexity of data protection, intellectual property rights, and algorithmic accountability, demands a coherent and harmonized regulatory reaction. But the current patchwork of country-level regulations generates legal fragmentation, hindering businesses and consumers who rely on cross-border digital transactions. This paper has addressed the key legal issues in regulating AI, including jurisdictional problems, data protection, intellectual property rights, algorithmic bias, and liability. In comparing the regulatory structures of prominent jurisdictions the European Union, the United States, and China this paper has addressed the merits and demerits of existing frameworks. Whereas the EU leads with overarching rules like the General Data Protection Regulation (GDPR) and the forthcoming AI Act, the U.S. adopts a more decentralized market model, and China's central model is testing privacy and surveillance.

In response to these challenges, there is an urgent need to pursue international collaboration in building homogenous, dynamic, and transparent legal frameworks to enable the accountable development and application of AI technology. Harmonizing the data protection legislation, establishing transparent standards for accountability of AI, and encouraging cross-border dialogue regarding intellectual property rights are necessary strides toward ensuring an equitable and secure digital marketplace. Moreover, international liability rules have to be designed to create crystal-clear lines of responsibility for the harm caused by AI, in order to make companies accountable for the effects their AI systems have on consumers and society.

To conclude, even though various regions are beginning to govern this,

a collective, global approach is required for addressing the complexities of AI on cross-border ecommerce. By promoting international cooperation, transparency, and fairness, we can establish a legality environment that not only encourages innovation, but consumer protection as well, as well as builds confidence in AI technologies. Lastly, international regulatory harmonization is the future in ensuring that AI can still unlock the potential of cross-border e-commerce while avoiding its risks.

REFERENCES

1. Bradford, A. (2023). The Brussels Effect in AI: How the EU shapes global AI regulation. Columbia Law Review, 123(5), 1201–1245. https://doi.org/10.7916/clr.v123i5.4512
2. Cath, C., & Wachter, S. (2024). Algorithmic auditing and the global governance of AI. Nature Machine Intelligence, 6(3), 102–115.
3. Qaiser, K., ur Rehman, I., & Naheed, S. (2025). The Future of Online Dispute Resolution in Cross-Border E-Commerce: Challenges and Opportunities. *Law Research Journal*, *3*(1).
4. Cimplifi. (2025). The updated state of AI regulations for 2025. https://www.cimplifi.com/resources/the-updated-state-of-ai-regulations-for-2025/
5. Dignum, V. (2024). Responsible AI: From principles to practice in cross-border contexts. Springer. https://doi.org/10.1007/978-3-031-56765-4
6. Zhu, J. (2021, October). Application analysis of artificial intelligence technology in the development of cross-border E-commerce. In *2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture* (pp. 1112-1116).
7. Dhabu, A. C. (2024). Legal Implications of Artificial Intelligence in Cross-Border Transactions-Navigating International Trade Law.G7 Hiroshima Process. (2023). International code of conduct for advanced AI systems. https://www.g7hiroshima.go.jp/en/ai-code
8. Gao, J., & Sheng, B. (2024). Cross-border data flow and digital trade: Domestic regulation and international rules. Journal of World Trade, 58(3), 401–422.
9. Gao, J., & Sheng, B. (2024). Fragmented governance: How AI disrupts traditional trade regulations. Global Policy, 15(3), 301–318. https://doi.org/10.1111/1758-5899.13245
10. Gürkaynak, G., et al. (2024). AI governance in a complex regulatory landscape. Computer Law & Security Review, 50, 105–123. https://doi.org/10.1016/j.clsr.2024.105789
11. Huang, X., & Wang, L. (2022). AI in cross-border logistics: Efficiency gains and liability gaps. International Journal of Electronic Commerce, 28(4), 567–589. https://doi.org/10.1080/12345678.2022.1234567
12. Shah, M. A. H., & Wu, X. (2024). Towards AI-Driven Trade Regulation: Regulatory Challenges and Global Commerce within WTO Framework. *Asian J. WTO & Int'l Health L & Pol'y*, *19*, 349.International Organization for Standardization. (2023). ISO/IEC 23053: Framework for AI system transparency (2nd ed.). https://www.iso.org/standard/81231.html
13. Khan, S., & Patel, R. (2025). Algorithmic bias in global hiring tools: A case study of jurisdictional conflicts. Ethics and Information Technology, 27(1), 88–104. https://doi.org/10.1007/s10676-024-09762-8
14. Li, M. (2023). China's state-led AI governance: Cybersecurity and surveillance priorities. Asian Journal of International Law, 13(2), 201–220.
15. Luo, Z. (2024). Data localization vs. global AI: The clash between GDPR and China's Cybersecurity Law. Harvard International Law Journal, 65(1), 134–159.
16. McKinsey Global Institute. (2023). The economic potential of generative AI: The next productivity frontier. https://www.mckinsey.com/generative-ai
17. National Institute of Standards and Technology (NIST). (2023). AI risk management framework (NIST AI 100-1). https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
18. Shah Jillani, M. A. H., & Wu, X. (2024). Towards AI-driven trade regulation: Regulatory challenges and global commerce within the WTO framework. Asian Journal of WTO & International Health Law and Policy, 19(2), 349–382. https://ssrn.com/abstract=4970263
19. Sharma, A. (2022). The Brussels Effect in AI regulation: Can the EU set global standards? European Law Review, 47(6), 789–810.
20. Sepehr Ghazinoory, Meysam Narimani, Faezeh Khamoushi & Hamid Kazemi (2017) Extracting the innovation policies for Iran based on the approximation of policy implications for comparative economic doctrines, Economic Research-Ekonomska Istraživanja, 30:1, 1257-1276, DOI: 10.1080/1331677X.2017.1311225
21. Basirat, Sepideh, Raoufi, Sadaf, Bazmandeh, Danial, Khamoushi, Sayeh and Entezami, Mahmoudreza (2025) Ranking of AI-Based Criteria in Health Tourism Using Fuzzy SWARA Method. Computer and Decision Making: An International Journal, 2 . pp. 530-545. ISSN 3008-1416
22. Saberi, R., & Sadeghi, S. (2022). The Future of Global E-Commerce Regulation: Legal Challenges in Ensuring Fair Competition, Consumer Rights, and Data Protection. *Legal Studies in Digital Age*, *1*(1), 39-52.
23. Zhang, Y. (2023). China's AI strategy: Surveillance, sovereignty, and the Digital Silk Road. China Quarterly, 255, 678–699.
24. Nawaser, K. (2015). Electronic commerce investment under condition of high uncertainty: a real options approach. In Academy of Management Proceedings (Vol. 2015, No. 1, p. 13682). Briarcliff Manor, NY 10510: Academy of Management.
25. Asadollahi, A., Jahanshahi, A. A., and Nawaser, K. (2011). A Comparative Study to Customer's Satisfaction from after Sales Services in the Automotive Industries. Asian Journal of Business Management Studies, 2(3), 124–134.
26. Hakkak, M., Nawaser, K., Jalali, M., Ghahremani, S., Vafaei-Zadeh, A., & Hanifah, H. (2023). Determining a model for eliminating organisational lying: a grounded theory approach. *International Journal of Information and Decision Sciences*, *15*(4), 345-365.
27. Yazdi, A., Nawaser, K., Pezeshgi, S., Mohsenifard, H., & Golamian, E. (2024). Artificial intelligence in social sustainability: A bibliometric and content analysis-based review. *Multidisciplinary Reviews*, (Accepted Articles).
28. Jafarkhani, F., Barani, F., Nawaser, K., Rashidi, H., & Gharleghi, B. (2024). Factors affecting the aesthetic experiences in educational games: A qualitative investigation. *Journal of Economy and Technology*, *2*, 200-207.
29. Yaghoubi, N. Khaksar, S.M.S. Banihashemi, S.A. Jahanshahi, A.A. Nawaser, K. (2011). The Impact of Knowledge Management on Customer Relationship Management European Journal of Economics, Finance and Administrative Sciences, (34), 76-86
30. Nawaser, K., Hakkak, M., Aeiny, M. A., Vafaei-Zadeh, A., & Hanifah, H. (2023). The effect of green innovation on sustainable performance in SMEs: the mediating role of strategic learning. International Journal of Productivity and Quality Management, 39(4), 490-511.
31. Nawaser, K., Jafarkhani, F., Khamoushi, S., Yazdi, A., Mohsenifard, H., & Gharleghi, B. (2024). The dark side of digitalization: A visual journey of research through digital game addiction and mental health. IEEE Engineering Management Review. Pp. 1 - 27 doi: 10.1109/EMR.2024.3462740.
32. Basit, S. A., Gharleghi, B., ur Rehman, A., Tee, P. K., Batool, K., & Nawaser, K. (2025). The Impact of Digital Products and Artificial Intelligence on Sustainable Marketing Methods. In *Managing Customer-Centric Strategies in the Digital Landscape* (pp. 1-24). IGI Global.
33. Seifi, N., Ghoodjani, E., Majd, S. S., Maleki, A., & Khamoushi, S. (2025). Evaluation and prioritization of artificial intelligence integrated block chain factors in healthcare supply chain: A hybrid Decision Making Approach. Computer and Decision Making: An International Journal, 2, 374–405. https://doi.org/10.59543/comdem.v2i.11029
34. Wang, L., & Zhu, Y. (2022). AI-powered customer service in global e-commerce: Opportunities and risks. Journal of Consumer Policy, 45(2), 245–268. https://doi.org/10.1007/s10603-022-09533-4