

Security risks and regulation of cross-border e-commerce in digital economy

Journal of
Electronic
Business & Digital
Economics

Shiqiang Wang

*School of Urban Economics and Public Administration, Capital University of
Economics and Business, Beijing, China*

Haoning Liu

School of Engineering, The University of Sydney, Sydney, Australia

Zhuonan Li

*School of Urban Economics and Public Administration, Capital University of
Economics and Business, Beijing, China, and*

Shu Zhang

Renmin University of China, Beijing, China

385

Received 7 December 2024

Revised 22 July 2025

Accepted 22 July 2025

Abstract

Purpose – “Security risks and regulation of cross-border e-commerce in digital economy” examines the key security threats – data breaches, payment fraud, logistics disruptions, product compliance and Internet Protocol protection – and develops a multi-layered governance framework to support platform operations and policymaking in the digital economy.

Design/methodology/approach – Drawing on the Web of Science Core Collection, we searched for literature published between January 2020 and October 2024 using keywords such as “cross-border e-commerce,” “global digital economy,” “data security risk,” “cross-border e-commerce data protection” and “cross-border data privacy regulation,” yielding 5,097 initial records. Using the ASReview active-learning tool, we screened out irrelevant studies (terminated after 20 consecutive irrelevant labels) to retain 226 high-relevance publications. We then applied CiteSpace for keyword co-occurrence and clustering analyses and conducted comparative case studies across five countries, supplemented by in-depth interviews with ten industry experts, forming a two-phase mixed qualitative and quantitative research design.

Findings – The study identifies significant security risks in cross-border e-commerce, including data breaches, payment fraud, logistics disruptions, product compliance issues and intellectual property challenges. Current regulatory frameworks help mitigate these risks but face hurdles in cross-border harmonization, technology deployment and operational consistency.

Originality/value – Integrating technical (blockchain and real-time artificial intelligence (AI) monitoring), legal (Standard Contractual Clauses and Data Protection Impact Assessments) and operational (multi-regional logistics and merchant vetting) dimensions, this paper proposes innovative measures – including unified data-sharing platforms and intelligent compliance modules – and advances a forward-looking framework incorporating generative AI and decentralized digital identity systems, offering concrete guidance for policymakers, regulators and practitioners.

Keywords Cross-border e-commerce, Data security, Regulatory compliance, Global collaboration, Digital economy, Bibliometrics, CiteSpace, Consumer trust

Paper type Research article

1. Introduction

With the rapid advancement of Internet technologies and the increasing integration of the global market, the digital economy has become a pivotal component of the global economic

© Shiqiang Wang, Haoning Liu, Zhuonan Li and Shu Zhang. Published in *Journal of Electronic Business & Digital Economics*. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at [Link to the terms of the CC BY 4.0 licence](#).

Funding: This work was supported by China Association of Higher Education (award number: Program No23JJ0101).



Journal of Electronic Business & Digital
Economics
Vol. 4 No. 2, 2025
pp. 385-401

Emerald Publishing Limited

e-ISSN: 2754-4222

p-ISSN: 2754-4214

DOI 10.1108/JEBDE-12-2024-0053

landscape. Centered on data and information technologies, the digital economy has not only facilitated the transformation and innovation of traditional economic models but has also significantly altered the dynamics of global trade. According to estimates from [eMarketer \(2020, 2023\)](#), the e-commerce market share is projected to increase by 45.8% over the next two years. Continued growth is anticipated, with the market share expected to reach 21.8% by 2024, representing a rise of 8.2% points over just five years. By 2025, this figure is expected to exceed \$7 trillion. Furthermore, the global cross-border e-commerce market continues to expand, with global retail e-commerce sales projected to reach nearly \$6 trillion in 2023 and surpass \$7 trillion by 2025.

The rapid development of cross-border e-commerce, a key component of the digital economy, has significantly facilitated international trade and enhanced global market integration. It has also provided both businesses and consumers with broad product choices and more convenient transaction methods. The number of global cross-border e-commerce buyers is growing rapidly, highlighting the significant market potential in this sector ([eMarketer, 2022](#)). As a key component of the digital economy, the rapid development of cross-border e-commerce not only facilitates international trade and enhances global market integration but also offers businesses and consumers a wider range of product choices and more convenient transaction methods. Emerging technologies such as big data analytics, artificial intelligence (AI), blockchain and cloud computing are continuing to drive cross-border e-commerce advancements, improving transaction efficiency and transparency, companies can expand their reach beyond local markets and increase their international market share.

With the widespread application of emerging technologies such as big data, AI, blockchain and cloud computing in cross-border e-commerce, new security risks and operational challenges have become increasingly apparent. Data security, being the core asset of cross-border e-commerce, is directly related to platform stability, consumer trust and the integrity of the global supply chain. According to [McKinsey & Company \(2020\)](#), companies face multiple challenges such as localization, logistics management and legal compliance when launching and operating these platforms. While the development of the Internet has boosted the number and speed of cross-border e-commerce transactions, it has also brought about problems such as data leakage, cyberattacks, payment fraud and counterfeit goods. These security risks not only infringe on consumers' rights and interests but also pose risks to merchants' operations and reputations. The [World Economic Forum \(2020\)](#) has noted that cybersecurity threats have become a global concern. Furthermore, there are significant differences in regulatory standards and laws for cross-border e-commerce exist among countries, and a unified global regulatory framework has yet to be established, making the global risk management of cross-border e-commerce more complex ([OECD, 2021](#)).

Against this backdrop, promoting cross-border e-commerce innovation while protecting data security has become a major issue for policymakers and industry participants. Data protection and privacy issues have sparked extensive discussions on the need to develop effective regulatory mechanisms. These mechanisms aim to address the challenges posed by technological advancements while ensuring the security and fairness of the cross-border e-commerce ecosystem. Therefore, exploring how to optimize the security and regulatory mechanisms of cross-border e-commerce, as well as assessing the effectiveness and inadequacies of existing policies, is crucial to ensure its healthy development of cross-border e-commerce.

In general, while existing studies have proposed some solutions from different perspectives when exploring the security risks and regulatory mechanisms of cross-border e-commerce, they still appear to be relatively one-sided and lack of systematicity. Therefore, this study aims to integrate the existing literature through CiteSpace analysis to propose a comprehensive solution for cross-border e-commerce security risks and regulation in the digital economy. This analysis will not only help identify the main issues and trends in current research but also provide empirical evidence and theoretical support for the development of more effective regulatory policies.

The research questions are as follows.

- (1) What are the main security risks and solutions of cross-border e-commerce?
- (2) What is the current regulatory status of governments and international organizations in cross-border e-commerce security and what are the future development trends?

The purpose of this paper is to explore the security risks of cross-border e-commerce and its regulatory mechanism in the context of digital economy, aiming to provide references for the practice and research in related fields. It is hoped that the relevant results obtained can be learner-centered and combined with the actual situation in China to form a solutions to the problems related to educational data ethics. The full paper is divided into three parts, as follows. (1) First, a bibliometric analysis of the existing literature is conducted. (2) Based on the existing literature, further bibliometric analysis is carried out to sort out the dilemmas and solutions to educational data ethics to sort out the dilemmas and solutions to educational data ethics in China. (3) The third part describes the conclusions and insights that can be drawn from this study.

2. Research methodology

2.1 Data source and data inclusion criteria

This study focuses on the security risk and regulation of cross-border e-commerce in the context of digital economy by using the Web of Science Core Collection as the data source. In order to ensure the relevance and comprehensiveness of the literature, this study used the following keywords for searching: “cross-border e-commerce,” “global digital economy,” “data security risk,” “cross-border e-commerce data protection” and “cross-border data privacy regulation.” The search covered academic papers, conference papers, online reviews and books between 2020 and October 2024, and a total of 5,097 preliminary search results were obtained. In order to improve the screening efficiency, this study introduced the ASReview software, to screen highly relevant literature to the topic in real time and prioritize the labeling of these documents. When 20 consecutive documents were labeled as irrelevant, the screening was stopped. Finally, 226 literature related to the study topic were screened (Figure 1).

The literature inclusion criteria are as follows: (1) Literature must address the security risks of cross-border e-commerce, including data leakage, payment fraud and other issues; (2) Legal frameworks or policy analyses related to cross-border e-commerce security regulation; (3) Articles examining the application of technology to cross-border e-commerce security risk management, such as blockchain technology, big data analytics and so on and (d. Case studies that provide regulatory strategies, exploring international cooperation and transnational regulatory frameworks.

2.2 Analytical framework

The analytical framework of this study combines bibliometric methods and qualitative analysis. Firstly, the literature screened by Q1 was analyzed bibliometrically using CiteSpace software, focusing on the identification of research hotspots, trends and co-occurring networks of key scholars and institutions. Through keyword co-occurrence network analysis, research trends and development paths of cross-border e-commerce security risk and regulation were identified. Secondly, based on the results of the Q1 bibliometric analysis, high-impact literature is analyzed in depth, and Q2 research is conducted to refine the core challenges and solution strategies of cross-border e-commerce in terms of data protection and privacy regulation.

Through the two-phase analysis, this study not only reveals the research hotspots and trends in the existing literature but also summarizes the practices and challenges faced by governments and international organizations in the field of cross-border e-commerce security regulation (e.g. Figure 2).

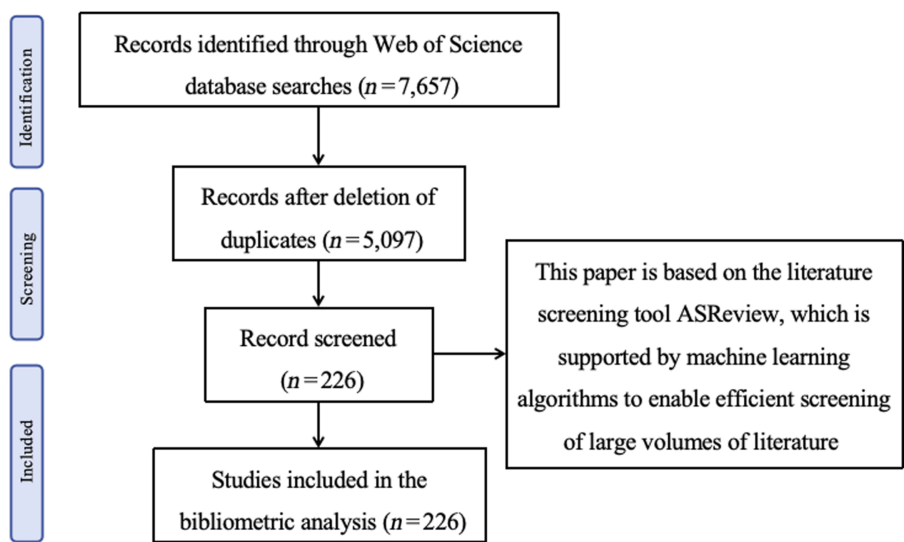


Figure 1. Flowchart of literature screening process. Literature screening was conducted based on literature screening criteria and literature screening tool (<https://asreview.nl/>). Figure by authors

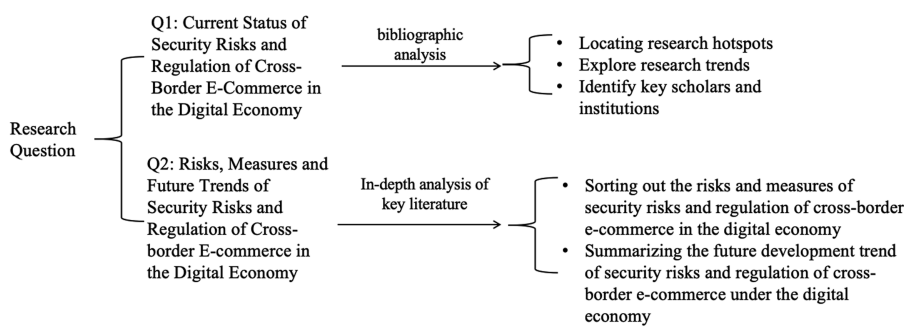


Figure 2. Research framework for the whole study

2.3 Bibliometric analysis of data ethics

Focusing on the theme of “security risks and regulation of cross-border e-commerce in the digital economy,” this paper constructs a keyword co-occurrence network by using CiteSpace to reveal the research hotspots of cross-border e-commerce security and regulation in recent years. Under the background of rapid development of the digital economy, cross-border e-commerce has become an important driving force to promote global trade, but it also brings challenges in various aspects such as data security, privacy protection and legal regulation, as shown in Figure 3, “#0 literature analysis,” “#1 regulated business mechanism,” “#2 comparative analysis,” “#3 sustainability risk management,” “#4 consumer protection,” “#5 AI,” “#6 global value chain,” “#7 global digital economy research” and other keywords co-occurring in the network based on the frequency of simultaneous appearance of the literature in different articles. The largest cluster is “#0 literature analysis,” which covers the most keywords in the cluster and contains 33 literature nodes, which mainly focuses on cross-border e-commerce research. In addition, the cluster “#5 AI” focuses on multidisciplinary research

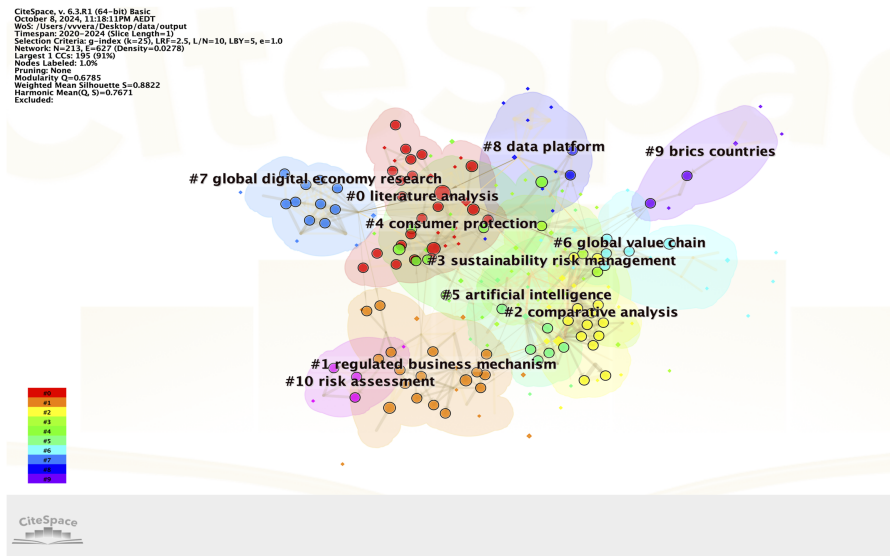


Figure 3. Keyword co-occurrence network, from 2020 to 2024 (first 11 clusters). Figure by authors

fields, and its average year is also 2020, which shows the rapid development trend of AI in business and management applications. As shown in the figure, the main research hotspots in this paper focus on “#1 regulated business mechanism,” “#5 AI,” “#4 consumer protection,” “#8 data platform” and other clusters, and these keywords reflect the multi-dimensional risk factors of cross-border e-commerce in the process of globalization.

It is worth noting that the different colored clusters in the figure show the correlation between the keyword clusters. For example, “#1 regulated business mechanism” and “#3 sustainability risk management” show high centrality in the research network. This suggests that they serve as bridges in interdisciplinary research, connecting multiple topics, especially in the context of data security and policy development. These research trends suggest that the current convergence of data science and business management is concerned not only with technological advances but also with the challenges of legal regulations and ethical risks.

Table 1 details the size, homogeneity and average year of publication for the different clusters. ClusterID denotes the cluster number, Size is the number of documents, Silhouette measures cluster quality, Label (LSI) extracts topics based on latent semantic indexing, Label (LLR) identifies statistically significant keywords using log-likelihood ratios, Label (MI) measures the relevance of a term to the cluster through mutual information and Average Year reflects the average publication year of the cluster. These keywords reflect the importance of topics such as cross-border e-commerce, data platforms, digital economy and data security in current research. The keyword characteristics and average year of publication for different clusters can be seen in Table 1. “#1 regulated business mechanism” is the core cluster of cross-border e-commerce security regulation, which contains keywords such as “cross-border data transfer,” “GDPR (EU General Data Protection Regulation),” etc., showing that researchers are highly concerned about privacy protection and data regulation in cross-border e-commerce data flow. In addition, the cluster “#5 AI” reflects the application of intelligent technology in cross-border e-commerce security, including intelligent data analysis and anomaly detection to improve the efficiency of risk identification.

Overall, with the rapid development of the digital economy, the data security risks in cross-border e-commerce have become more and more prominent, requiring more perfect regulatory

Table 1. Summary of the largest 11 clusters

ClusterID	Size	Silhouette	Label (LSI)	Label (LLR)	Label (MI)	Average year
0	33	0.809	Cross-border e-commerce research trend	Literature analysis (34.79, 1.0E−4)	Future research direction (1.08)	2020
1	27	0.787	Digital age	Regulated business mechanism (35.42, 1.0E−4)	Cross-border data transfer (0.28)	2021
2	24	0.963	Digital economy	Comparative analysis (34.21, 1.0E−4)	G20s digitalization leadership (1.27)	2020
3	23	0.789	Sustainability risk management	Sustainability risk management (24.93, 1.0E−4)	South Africa (0.43)	2021
4	19	0.929	Consumer protection	Consumer protection (30.39, 1.0E−4)	Risk assessment (0.37)	2020
5	17	0.907	Artificial intelligence	Artificial intelligence (50.15, 1.0E−4)	Sports industry (0.3)	2020
6	16	0.92	Digital platform	Global value chain (30.85, 1.0E−4)	Competition policy (0.14)	2020
7	14	0.989	Empirical analysis	Global digital economy research (19.82, 1.0E−4)	Risk assessment (0.04)	2021
8	11	0.954	Using metadata	Data platform (25.12, 1.0E−4)	Risk assessment (0.03)	2020
9	6	0.964	BRICS countries	BRICS countries (18.84, 1.0E−4)	GDPR (0.02)	2020
10	5	0.985	Cross-border data security from the perspective of risk assessment	Risk assessment (11.76, 0.001)	Digital economy (0.03)	2021

Source(s): Table by authors

mechanisms. In the keyword co-occurrence network, “#3 sustainability risk management” and “#6 global value chain” are closely connected. This suggests that the security risk of cross-border e-commerce is not only limited to the data itself but also involves the management and synergy of the supply chain. Therefore, the regulation of cross-border e-commerce requires not only the support of technical means but also the strengthening of international cooperation and the formulation of standardized laws and regulations so as to safeguard data security and consumer rights and interests on a global scale.

2.4 Research analysis of scholars and institutions

In order to draw further conclusions from the above demonstration results, it is necessary to analyze the mutual relations between research institutions and scholars. In order to identify the scholars who have had a significant influential role in the topic of security risk and regulation of cross-border e-commerce in the digital economy in the last five years, this study formed a collaborative network of authors based on CiteSpace, as shown in Figure 4 and counted the papers published by six scholars in the last five years, as shown in Table 2.

The booming development of cross-border e-commerce in the digital economy has brought new opportunities for global trade while also exposing many security risks and regulatory challenges. Liu (2020) proposes the use of blockchain technology to improve information

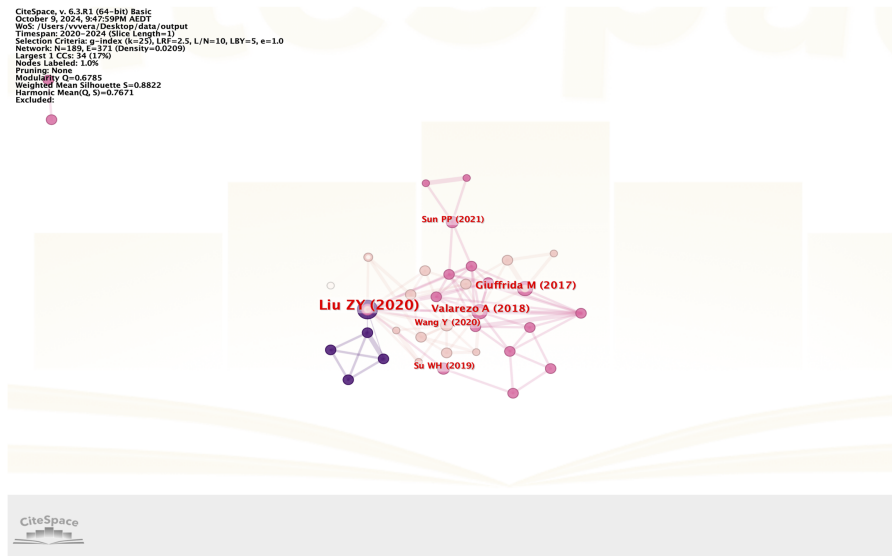


Figure 4. Author co-occurrence network, from 2020 to 2024 (first 6 clusters). Figure by authors

Table 2. The top 6 scholars' publications in the past 10 years

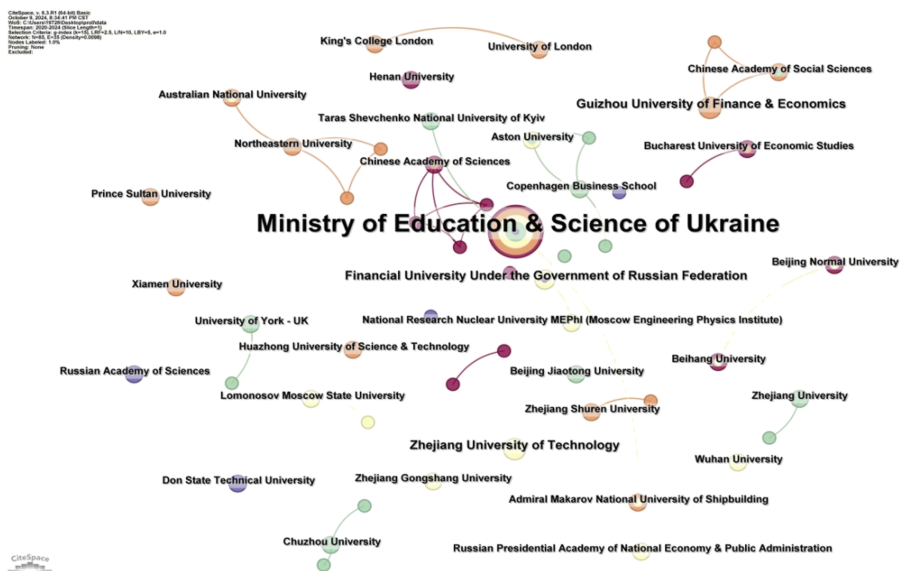
S/ N	Scientific scholars	Number of publications	Time of initial publication year
1	Liu ZY	8	2020
2	Valarezo A	4	2018
3	Giuffrida M	4	2017
4	Sun PP	3	2021
5	Wang Y	3	2020
6	Su WH	3	2019

Source(s): Table by authors

transparency and security in cross-border e-commerce, especially for the risk of information asymmetry and data tampering. Similarly, [Sun \(2021\)](#) emphasizes the role of Internet of Things (IoT) technology in regulatory system optimization to reduce the risk of illegal goods circulation and data fraud through real-time monitoring of logistics flows. In addition, logistics occupies a key position in the operation of cross-border e-commerce, and [Giuffrida, Mangiaracina, Perego, and Tumino \(2017\)](#) analyze the role of logistics in facilitating or hindering e-commerce development, noting that logistical failures can lead to risks such as supply chain disruptions and customer information leakage.

From a regulatory perspective, [Valarezo \(2018\)](#) reveals that consumer concerns about cybersecurity and privacy protection are among the main obstacles limiting the development of cross-border e-commerce. [Wang \(2020a\)](#) pointed out that e-commerce companies need to effectively manage logistics, information flow and capital flow to cope with compliance risks in cross-border transactions. Additionally, [Wang \(2020b\)](#) further shows that cross-border e-commerce under the transaction cost analysis framework has a significant impact on China's international trade, but compliance costs and regulatory loopholes may bring about trade

In terms of public policy and education, [Voronkova, Nikitenko, and Vasylychuk \(2023\)](#) examine the practical experiences of different countries in the digital transformation of education, noting that the digitization of the education system is essential for adapting to the future economic environment. Similarly, [Lukianenko, Lukianenko, Mozghalli, Dvornyk, and Oriekhov \(2020\)](#) show that the digital transformation of the activities of higher education



Downloaded from <ftp.nowpublishers.com/jebde/article-pdf/4/2/385/10576679/jebde-12-2024-0053en.pdf> by guest on 11 August 2026

Table 3. Institutions that have published the most papers in the last 5 years

S/ N	Number of publications	Year	Institution
1	16	2020	Ministry of Education and Science of Ukraine
2	3	2022	Zhejiang University of Technology
3	3	2023	Guizhou University of Finance & Economics
4	3	2020	Financial University Under the Government of Russian Federation
5	2	2021	Aston University
6	2	2023	Bucharest University of Economic Studies
7	2	2021	Beijing Jiaotong University
8	2	2022	Wuhan University
9	2	2023	University of London
10	2	2020	Russian Academy of Sciences
11	2	2021	Chuzhou University
12	2	2021	Zhejiang University
13	2	2022	Beijing Normal University
14	2	2021	Taras Shevchenko National University of Kyiv
15	2	2023	Xiamen University
16	2	2021	Chinese Academy of Social Sciences
17	2	2023	Northeastern University
18	2	2024	Henan University
19	2	2023	King's College London
20	2	2022	Australian National University
21	2	2021	University of York – UK
22	2	2021	Copenhagen Business School
23	2	2022	Lomonosov Moscow State University
24	2	2023	Chinese Academy of Sciences
25	2	2020	Don State Technical University
26	2	2022	National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
27	2	2023	Prince Sultan University
28	2	2022	Beihang University
29	2	2023	Huazhong University of Science and Technology
30	2	2022	Admiral Makarov National University of Shipbuilding
31	2	2023	Zhejiang Shuren University
32	2	2022	Zhejiang Gongshang University
33	2	2022	Russian Presidential Academy of National Economy and Public Administration

Source(s): Table by authors

institutions has become an important strategy for improving the competitiveness of today's educational institutions.

Furthermore, [Irtysheva, Kim, and Kletsov \(2022\)](#) and [Diugowanets \(2020\)](#) show that companies and countries need to harmonize global and local digitalization strategies in order to ensure sustainable development in the international market. Particularly in the current geopolitical context, [Spitsina et al. \(2022\)](#) reveal how Ukraine can contribute to the sustainable development of the country through digitization in the context of military conflict.

The Ministry of Education & Science of Ukraine also explores the trends of e-commerce and digital trade. [Volkova, Kuzmuk, Oliinyk, Klymenko, and Dankanych \(2021\)](#) and [Shevchenko \(2023\)](#) point out that e-commerce and digital trade have become key drivers of global economic growth and that well-developed digital networks and payment systems are particularly important for the success of international trade.

As a result, scholars have concentrated on research focusing on digital transformation in business, public policy and education, in line with the clusters of focus summarized in the previous section.

3. Key risks and countermeasures in cross-border e-commerce

3.1 Data security and privacy risks

Data leakage has become a common and serious problem in cross-border e-commerce. As e-commerce platforms handle large amounts of sensitive consumer information – such as payment records and personal addresses – cybercriminals often attack servers or payment systems to steal data. Such information breaches can lead to the compromise of consumers' financial accounts and damage the platform's reputation. For example, in 2021, a massive data breach occurred on the Facebook platform, resulting in the exposure of users' personal information. The compromised information included details such as users' names, phone numbers, emails, birthdays and geographic locations. This incident triggered a wide-ranging discussion on privacy protection and data security regulation globally and led the relevant countries to strengthen fines and regulation concerning data breaches. Such incidents not only increase the financial risks for users but may also lead to lawsuits.

In addition, differences in privacy protection regulations across countries exacerbate the complexity of compliance management. For example, the EU's GDPR has become one of the data protection standards, and the GDPR requires companies to adopt mechanisms such as Standard Contractual Clauses and Data Protection Impact Assessments to safeguard compliance for cross-border data transfers (Pandectes, 2023) and companies that fail to comply with the GDPR regulations may face severe penalties. This is because there are inconsistencies in data regulations in different jurisdictions, such as differences in privacy and data control requirements between the California Consumer Privacy Act (CCPA) and the GDPR.

Further complicating matters is the high incidence of data misuse. Some cross-border e-commerce and social media platforms use user behavior data for precision marketing by selling it to advertisers and partner companies. However, this practice often violates consumers' privacy rights. User behavior data, including access logs, browsing history, and shopping habits, are used to construct personalized advertisements, but the process lacks transparency and makes it difficult to obtain informed consent from users (Termly, 2023). The GDPR makes it clear that this type of data processing requires the active consent of the user; otherwise, it constitutes a privacy violation. The regulation also requires companies to provide users with the right to refuse the sale of data and guarantees users the right to request the deletion of their personal data. Similarly, the CCPA grants users the right to opt out of precision advertising, and these legal frameworks aim to balance the tension between business interests and user privacy (Termly, 2023). However, despite these regulations, some companies still employ strategies to circumvent their legal obligations and trade data through vague terms. Such behavior not only increases legal risks but may also lead to decreased user trust and damage to corporate reputation.

To mitigate data security and privacy risks, cross-border e-commerce platforms can effectively cope with the data security and privacy risks by implementing comprehensive measures at the technical, legal and user levels. These measures aim to protect the security of users' data, enhance users' trust in the platforms and promote the sustainable development of the platforms. At the technical level, enterprises not only need to technically encrypt data to ensure data security during storage and transmission but also need to establish data protection officers within the organization to oversee compliance and pass international certifications to enhance trust and transparency. Platforms should also establish strict access control mechanisms to limit access to user data and conduct regular security audits to identify and fix security vulnerabilities in a timely manner to prevent data leakage incidents. In addition, security awareness training for employees should be strengthened to raise their awareness of data security and privacy protection and to prevent data leakage caused by employee operational errors. In addition, at the legal level, platforms should comply with national data protection regulations, such as GDPR and CCPA, to ensure compliance of cross-border data transfer. Sign a data protection agreement with a third-party partner to clarify the responsibilities and obligations of both parties in terms of data security and establish a

cooperation mechanism and data protection system responsible for supervising and managing data security within the enterprise. Specifically, at the user level, platforms should obtain informed consent from users before collecting and using their data, informing them about how their data will be used and the protection measures in place. They should provide options for user privacy settings that allow users to control how their personal information is collected and utilized. Additionally, disclosing the enterprise's data protection policies to users can enhance their trust in the platform.

3.2 *Payment and transaction risks*

Due to the complexity of cross-border payments, payment fraud has become a major challenge for businesses and consumers, especially in multi-currency transactions where such fraud is more frequent. Payment fraud is on a significant rise globally and is particularly prevalent in the cross-border payments environment of multi-currency transactions. According to Statista, fraud rates for businesses have risen significantly in recent years, with global e-commerce payment fraud losses growing year-over-year from approximately \$17bn in 2020 to a projected \$48bn in 2023. [Sandoval, de Almeida Vau, Solaas, and Rodrigues \(2024\)](#) pointed out that criminals use deepfakes to synthesize identity documents, forge video evidence and carry out “voice phishing” scams, exacerbating the risk of identity theft and financial fraud. This has brought new challenges to the security and regulation of cross-border e-commerce in terms of identity review and payment risk control. These frauds include credit card information theft, fraudulent payments, account takeovers and phishing attacks ([Statista, 2023](#)). At the same time, the rollout of decentralized identity (DID) faces rollout bottlenecks such as missing standards for share management, difficulties in cross-chain interoperability and regulatory compliance challenges ([Casino, Dasaklis, & Patsakis, 2019](#)). To combat these risks, organizations need to employ multiple layers of protection, including two-factor authentication (2FA), payment gateway encryption and real-time transaction monitoring. In recent years, there has been a rise in emerging technologies such as generative AI (e.g., OpenAI's ChatGPT) and blockchain digital identity (DID), which have far-reaching implications for the regulation and security of cross-border e-commerce. On the positive side, ChatGPT and other emerging technologies are used in cross-border e-commerce product selection, content production, multilingual real-time customer service, etc. The rapidity of content production, the convenience of interaction and the simplification of work can greatly enhance the delivery efficiency of cross-border e-commerce. In terms of blockchain digital identity, blockchain DID technology provides cross-border e-commerce with a convenient means of identity verification, which is expected to reduce the cost of trust and the risk of fraud ([Kuperberg, 2020](#)). According to a study in the United Nations Centre for Trade Facilitation and Electronic Business white paper (2022), the combination of virtual currency decentralization with authenticated VCs enables the verification of digital identities, improves efficiency and reduces uncertainty, enables transparency in sustainable and ethical supply chains and helps to combat illegal imports, tax evasion and border risks. In addition, Know Your Business processes play an important role in preventing account takeovers and other forms of payment fraud by rigorously verifying the legitimacy of business partners. Countries are also strengthening the regulation of payment systems, promoting the adoption of standards such as International Organization for Standardization 20022 to facilitate the transparency of payment data. This standardized communication format helps to enhance collaboration between banks and financial institutions and improve anti-fraud capabilities and regulatory compliance. These measures not only improve the efficiency of payment systems but also ensure the reliability of transactions, creating a safer cross-border payment environment for businesses and consumers.

Another key issue is fraudulent orders and malicious refunds, which are common problems on e-commerce platforms. Unscrupulous individuals create fake transactions and exploit refund policies to obtain illegitimate gains. This fraudulent behavior not only leads to financial losses

for merchants but also may damage the platform's reputation. According to LiquiDonate's analysis, losses due to returns and refund fraud have reached \$101bn in 2023, accounting for more than 10% of all returns. Common malicious behaviors include "rental purchases" (i.e. temporarily using an item and then returning it), price fraud using discounted items, and requesting refunds using forged or stolen vouchers. To combat such fraud, platforms need to use big data and AI technologies to monitor transaction behavior. These technologies can help identify unusual transaction patterns in a timely manner and stop fraudulent orders and improper refunds from occurring. Platforms can also reduce the risk of fraud by enhancing the transparency of return and refund policies, adopting real-time monitoring systems and introducing mechanisms to refund only store credits rather than cash refunds.

3.3 Logistics and supply chain risks

Cross-border e-commerce logistics networks often experience disruptions due to uncontrollable factors such as natural disasters, political situations and global epidemics, which can cause delays in shipments and affect the normal functioning of the supply chain. The global blocking measures during the 2020 New Crown epidemic backlogged a large number of orders, which seriously exposed the vulnerability of the supply chain in responding to unforeseen events (McMaster, 2020). This phenomenon suggests that enterprises must improve supply chain resilience and ensure stability and flexibility of logistics through multi-supplier cooperation and regionalized logistics layout. According to the survey, supply chain technology is crucial in improving the resilience of organizations. The application of real-time monitoring, AI and blockchain technology enables enterprises to better cope with uncertainty in the supply chain and improve the transparency and efficiency of logistics operations. In addition, enhanced collaboration with suppliers and logistics partners can help reduce bottlenecks and improve customer satisfaction (Zhitao, Elomri, Kerbache, & El Omri, 2020). Resilience, agility and digital transformation will be key factors in future supply chain strategies. Companies will need to adopt smart technologies and new processes, such as dynamic inventory management and automated systems, to ensure that they are able to quickly adjust their operations when the next crisis occurs, reducing the impact on the global supply chain (EY, 2023).

Cross-border e-commerce logistics networks face complex challenges, including not only uncontrollable factors but also the impact of customs clearance procedures and tariff differences. Logistics disruptions during global epidemics led to large backlogs of orders, highlighting the lack of supply chain resilience, which prompted firms to increase collaboration with regional logistics partners to enhance their ability to cope with future emergencies (Alicke et al., 2022). Cross-border logistics risks are further exacerbated by the complexity of the customs clearance process and differing customs clearance regulations across countries. The firms should contend with inconsistent tariff policies and cumbersome paperwork, which not only increases transportation costs but can also lead to delayed or even returned shipments, which undermines the platform's price competitiveness (Kuehne & Nagel, 2023). To improve logistics efficiency and reduce delays and uncertainty, companies are turning to the application of IoT and blockchain technologies to enable full-process tracking and dynamic management of goods. These technologies can provide greater transparency and control, helping companies optimize their supply chains and enhance the customer experience. Moving forward, it will be key to drive logistics standardization and digital reforms through synergistic collaboration with government and industry partners. These initiatives will further reduce cross-border compliance barriers and support sustainable development in the global marketplace.

3.4 Product compliance and quality risks

Cross-border e-commerce companies face products' quality and compliance issues as they expand globally. For example, in 2022, Amazon and the China Association for Consumer Products Quality and Safety Promotion co-hosted the "2022 Export Consumer Goods Safety

and Compliance Annual Wrap-up Conference,” which reviewed the year’s work on product quality and compliance and recognized outstanding compliance service providers, according to PRNewswire. Some products fail to meet the quality standards of importing countries, resulting in a compromised consumer experience and weakening the platform’s reputation. CIFNEWS reported in 2023 that Amazon has strengthened its review of sellers’ product compliance, especially scrutinizing the authenticity of Children’s Product Certificate. Sellers found to have false certificates are at risk of having their stores blocked. These incidents show that Amazon has continued to focus on and strengthen product quality and compliance management during its global expansion to safeguard consumer rights and platform reputation.

Research has pointed out that consumers are increasingly expecting higher levels of product quality and service, especially in transactions involving different countries and that cultural differences can also affect consumer satisfaction with products and services (Han & Han, 2023). To address these challenges, platforms should scrutinize the qualifications of the onboard merchants and conduct thorough quality testing of their goods to ensure compliance with the standards of importing markets. In pursuit of this end, platforms need to work closely with international regulators to establish reliable product traceability systems through blockchain technology. These systems can ensure transparency in the origin of products and allow consumers and platforms to verify the authenticity of goods before transactions, effectively preventing the spread of counterfeiting (Lee & Yeon, 2021). In addition, blockchain provides tamper-proof records in supply chain management, and this transparency helps combat fraud and enhances consumer trust. E-commerce platforms also need to adopt stringent screening mechanisms, take severe measures against non-compliant merchants, including permanently blocking non-compliant accounts and establish efficient complaint and customer service systems to ensure that consumers’ interests are protected. These measures not only enhance consumer experience but also improve brand image and platform competitiveness (Lee & Yeon, 2021). In addition, the application of technologies such as the IoT can further enhance the transparency of product tracking and quality management, helping platforms to reduce the risk of the distribution of non-compliant goods and improve overall market competitiveness (Zhitao *et al.*, 2020).

Intellectual property disputes constitute one of the major challenges facing cross-border e-commerce platforms. Unauthorized sales of branded products by some merchants not only harm the interests of the brand owners but also increase the legal risks for the platforms. Trademark infringement and copyright disputes present a complex scenario across multiple jurisdictions, and the differences in Internet Protocol (IP) regulations between different countries also make compliance efforts for businesses (Flatfee, 2023). To address these issues, platforms should strengthen their vetting processes for merchants and products, enhance their reward and penalty systems by imposing stricter sanctions and ensure compliance with the intellectual property regulations of importing countries. Collaboration with international organizations is crucial to establishing effective global IP protection mechanisms. For example, by working with regulators and brands, platforms can reduce the incidence of infringement. In addition, adopting technologies such as blockchain to establish a product traceability system can reduce the circulation of counterfeit goods by increasing transparency and ensuring that the origin of goods is legitimate and traceable. Platforms also need to establish efficient complaint-handling mechanisms to ensure that consumers can get timely help when they encounter problems. These measures not only protect consumers’ rights and interests but also enhance the platform’s credibility and competitiveness in the market, laying the foundation for long-term development in the global market (Flatfee, 2023).

4. Summary

Cross-border e-commerce has brought market expansion and internationalization opportunities for enterprises in the process of promoting global trade. However, the analysis in this paper shows that cross-border e-commerce also faces multiple security and

regulatory challenges, including data leakage and payment fraud. To address these challenges, it is necessary to build a comprehensive regulatory system covering data security, payment management, product compliance monitoring and supply chain optimization.

4.1 Key findings

This study identifies the main security risks and regulatory challenges facing cross-border e-commerce in the digital economy environment, and the key findings include the following. Firstly, data security and privacy protection are core issues for cross-border e-commerce, with data leakage, payment fraud and privacy abuse becoming increasingly serious, while differences in data protection regulations (e.g. GDPR and CCPA) between different countries increase the complexity of compliance for businesses. Secondly, payment and transaction security is a huge challenge, with fraudulent behavior such as credit card theft, account takeovers and malicious refunds occurring frequently, and studies have shown that real-time transaction monitoring and identity verification using AI and machine learning technologies can effectively reduce risks. In addition, logistics and supply chain management remain weak links in cross-border e-commerce operations. Global epidemics, political uncertainty and supply chain disruptions have led to the need for companies to improve supply chain resilience, rely on multi-regional partners and leverage blockchain and IoT technologies to improve logistics transparency and efficiency. Product compliance and quality are also key issues, with some merchants facing compliance risks because they do not meet the quality standards of importing countries. The study recommends establishing product traceability systems and strengthening merchant audits and quality testing to ensure market competitiveness. Finally, the challenge of global regulatory harmonization remains, as companies have to deal with different legal requirements when operating across borders due to inconsistent standards in data protection, tax policies and e-contract enforcement across countries, and the study highlights the need to promote globally harmonized regulatory frameworks in order to reduce compliance barriers and enhance market transparency. These findings provide a systematic understanding of the sustainable development of cross-border e-commerce and provide a reference point for policymakers and businesses.

4.2 Research contribution

This study makes important contributions at the theoretical, practical and policy levels. In terms of theory, based on CiteSpace bibliometric analyses, this study systematically sorts out the research hotspots of cross-border e-commerce security and regulation, identifies the key topics of data security, payment fraud, logistics management and legal compliance and reveals the future research trends, which provides a comprehensive research framework for the academic community and fills in the systematic deficiencies in the existing research. In addition, this study builds a multi-level solution for cross-border e-commerce security management, proposing feasible practical strategies from multiple dimensions, including technology, law and operations, to provide practical guidance for enterprises to develop security and compliance management programmes in the complex global market environment. These strategies include strengthening data encryption and privacy protection, adopting AI technology for payment fraud prevention, optimizing supply chain resilience and establishing a global product compliance traceability system, which help enterprises to enhance security while maintaining market competitiveness. Meanwhile, the policy contribution of this study is reflected in the proposal to promote a globally harmonized regulatory framework for cross-border e-commerce, emphasizing intergovernmental cooperation, the construction of a data-sharing mechanism and the development of intelligent compliance tools in order to reduce cross-border trade barriers, improve regulatory efficiency and promote fair competition in the global market. Through this study, policymakers can better understand the current challenges of cross-border e-commerce

security regulation and provide references for the development of better and more operational international rules, thus promoting the sustainable development of the digital economy.

4.3 Future development

Looking ahead, cross-border e-commerce platforms need to strengthen data protection through encrypted storage and transmission technologies to prevent data leakage and privacy abuse issues. The implementation of a real-time monitoring system can help platforms detect suspicious behavior and quickly respond to potential risks. Additionally, payment systems should adopt dual identity verification and AI-driven anti-fraud technologies to effectively identify fraudulent transactions and malicious refunds and safeguard the security of transactions.

This study not only makes important contributions at the theoretical, practical and policy levels but also provides forward-looking insights into future evolutionary trends in cross-border e-commerce security and regulation. With the rapid development of emerging technologies such as generative AI and digital identity systems (DIS), the security and regulatory environment of cross-border e-commerce will face new opportunities and challenges. The application of Generative AI will greatly improve the risk identification and defense capabilities of e-commerce platforms. For example, through AI-driven intelligent customer service, transaction fraud detection and personalized security policies, platforms can identify abnormal transaction behaviors in real time and provide more accurate security protection. However, this technology could also be used by unscrupulous individuals to generate false product information, fraudulent user reviews or even synthetic identities, increasing the complexity of regulation. In addition, the proliferation of DIS, such as DID and blockchain-powered authentication technologies, is expected to enhance the trustworthiness of cross-border transactions and reduce identity theft and fraud, while streamlining the cross-border compliance process and enabling national regulators to track and manage user data more effectively. However, the implementation of these technologies has yet to face the inconsistency of global data privacy regulations and the harmonization of technical standards. Therefore, this study emphasizes that future regulation of cross-border e-commerce should accelerate the integration with new technologies and promote policy innovation and international cooperation, in order to ensure data security while facilitating the sustained and healthy development of the digital economy.

To achieve long-term stable growth, international cooperation between governments and businesses is crucial. Establishing a unified regulatory framework and standardized policies can reduce compliance barriers between countries, streamline cross-border business processes and enhance market sustainability. The Organization for Economic Co-operation and Development stresses the need for the international community to work together to promote the development of the digital economy, especially in terms of data protection and marketplace security, and that collaboration will improve the transparency of the global marketplace and the competitiveness of businesses. Furthermore, the study should expand the discussion on how to adapt the proposed security and regulatory framework to developing economies, which often face challenges such as limited regulatory capacity, weaker infrastructure and scarce technological resources. Tailoring flexible compliance strategies and technical solutions to meet these differentiated needs, while fostering regional cooperation and capacity building, is crucial to ensuring the security and inclusiveness of global cross-border e-commerce.

Moreover, platforms must continuously optimize logistics and supply chain management to mitigate the impact of uncontrollable external factors on operations. Building diversified supply chain partnerships and regionalized logistics networks will bolster the resilience of enterprises against unforeseen events such as natural disasters, political instability and epidemics. These measures will not only improve supply chain stability but also enhance consumer satisfaction and trust.

References

- Alicke, K., Barriball, E., Foster, T., Mauhourat, J., & Trautwein, V. (2022), "Taking the pulse of shifting supply chains", McKinsey & Company, 26 August.
- Baltgailis, J., Simakhova, A., & Buka, S. (2023). Digital currencies and fintech innovation technologies for economic growth. *Marketing i Menedžment Inovacij*, 14(3), 202–214. doi: [10.21272/mmi.2023.3-18](https://doi.org/10.21272/mmi.2023.3-18).
- Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. doi: [10.1016/j.tele.2018.11.006](https://doi.org/10.1016/j.tele.2018.11.006).
- Diugowanets, O. (2020). The role of digitalization in global and national economies.
- eMarketer (2020). Worldwide retail ecommerce forecast 2020. Available from: <https://www.emarketer.com/content/worldwide-ecommerce-continues-double-digit-growth-following-pandemic-push-online>
- eMarketer (2022). Worldwide retail ecommerce forecast 2022. Available from: <https://www.emarketer.com/insights/worldwide-ecommerce-sales-to-top-7-trillion/>
- eMarketer (2023). Worldwide retail ecommerce forecast 2023. Available from: <https://www.emarketer.com/chart/265660/retail-ecommerce-sales-worldwide-2021-2027-trillions-change-of-total-retail-sales>
- EY (2023). How COVID-19 impacted supply chains and what comes next. Available from: <https://www.ey.com>
- Flatfee (2023), "Common legal challenges for cross-border e-commerce", Flatfeecorp.com, 22 June.
- Giuffrida, M., Mangiaracina, R., Perego, A., & Tumino, A. (2017). Cross-border B2C e-commerce to greater China and the role of logistics: A literature review. *International Journal of Physical Distribution and Logistics Management*, 47(9), 772–795. doi: [10.1108/ijpdlm-08-2016-0241](https://doi.org/10.1108/ijpdlm-08-2016-0241).
- Han, L., & Han, X. (2023). Improving the service quality of cross-border e-commerce: how to understand online consumer reviews from a cultural differences perspective. *Frontiers in Psychology*, 14, 1137318. doi:[10.3389/fpsyg.2023.1137318](https://doi.org/10.3389/fpsyg.2023.1137318).
- Irtysheva, I., Kim, V., & Kletsov, Y. (2022). Managing business processes in the conditions of the development of the digital economy: Global and national experiences. *Baltic Journal of Economic Studies*, 8(5), 101–107. doi: [10.30525/2256-0742/2022-8-5-101-107](https://doi.org/10.30525/2256-0742/2022-8-5-101-107).
- Karp, S. (2024). Reengineering business operations within the digital economy.
- Khanin, I., Bilozubenko, V., & Sopin, Y. (2022). Improving the level of economic effectiveness of electronic payment services in a global digital economy. *Baltic Journal of Economic Studies*, 8 (1), 148–158. doi: [10.30525/2256-0742/2022-8-1-148-158](https://doi.org/10.30525/2256-0742/2022-8-1-148-158).
- Kuehne & Nagel (2023). E-Commerce logistics: Cross-border solutions. Available from: <https://home.kuehne-nagel.com>
- Kuperberg, M. (2020). Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. *IEEE Transactions on Engineering Management*, 67(4), 1008–1027. doi: [10.1109/TEM.2019.2926471](https://doi.org/10.1109/TEM.2019.2926471).
- Lee, H., & Yeon, C. (2021). Blockchain-based traceability for anti-counterfeit in cross-border e-commerce transactions. *Sustainability*, 13(19), 11057. doi:[10.3390/su131911057](https://doi.org/10.3390/su131911057).
- Liu, Z. Y. (2020). A blockchain-based framework of cross-border e-commerce supply chain. *Journal of Supply Chain Management*, 56(2), 112–125.
- Lukianenko, I., Lukianenko, O., Mozghalli, O., Dvornyk, I., & Oriekhov, M. (2020). Digital imperative of university activities transformation.
- McKinsey & Company (2020). China cross-border E-commerce market research white paper. Available from: <https://www.mckinsey.com.cn/中国跨境电商市场研究白皮书/>
- McMaster, D. (2020). *Impact of COVID-19 on global supply chains and E-commerce logistics*. UiT. Available from: <https://munin.uit>

- OECD (2021). Unpacking E-commerce. Available from: <https://www.oecd-ilibrary.org/>
- Pandectes (2023). Cross-border data transfer under GDPR: How to ensure compliance. Available from: <https://www.pandectes.io>
- Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*, 13(1), 41. doi: [10.1186/s40163-024-00239-1](https://doi.org/10.1186/s40163-024-00239-1).
- Shevchenko, A. (2023). Digital trade in global markets.
- Spitsina, L., Plukar, L., Maslyhan, O., Moroz, T., Kasmin, D., & Nazarenko, I. (2022). Digitalization of the economy as a factor of sustainable state development against the background of large-scale military aggression (Ukrainian experience).
- Statista (2023). E-commerce payment fraud losses worldwide from 2020 to 2023. Available from: <https://www.statista.com>
- Su, W. H. (2019). Creating a sustainable policy framework for cross-border E-commerce in China. *Asian Business and Management*, 18(3), 250–270.
- Sun, P. P., & Gu, L. (2021). Optimization of cross-border e-commerce logistics supervision system based on Internet of Things technology. *Journal of Internet Commerce*, 20(1), 45–60. doi: [10.1155/2021/4582838](https://doi.org/10.1155/2021/4582838).
- Termly (2023). Is behavioral advertising compliant with data privacy laws?. Available from: <https://www.termly.io>
- Valarezo, A. (2018). Drivers and barriers to cross-border e-commerce: Evidence from Spanish individual behavior. *Journal of Global Marketing*, 31(3), 170–182.
- Volkova, O., Kuzmuk, I., Oliinyk, N., Klymenko, I., & Dankanych, A. (2021), “Development trends of the digital economy: E-business, e-commerce”, *International Journal of Computer Science and Network Security*.
- Voronkova, O., Nikitenko, V., & Vasylychuk, G. (2023). Foreign experience in implementing digital education in the context of digital economy transformation, *Baltic Journal of Economic Studies*, 9(3), 56–65. doi: [10.30525/2256-0742/2023-9-3-56-65](https://doi.org/10.30525/2256-0742/2023-9-3-56-65).
- Wang, Y. (2020a). Cross-border e-commerce firms as supply chain integrators: The management of three flows. *Supply Chain Forum: International Journal*, 21(2), 156–165.
- Wang, Y. (2020b). The effect of cross-border E-commerce on China’s international trade: An empirical study based on transaction cost analysis. *Journal of Asian Economics*, 67, 101–115.
- World Economic Forum (2020). The global risks report 2020. Available from: <https://www.weforum.org/reports/the-global-risks-report-2020>
- Zhitao, Xu., Elomri, A., Kerbache, L., & El Omri, A. (2020). Impacts of COVID-19 on global supply chains: Facts and perspectives, *IEEE Engineering Management Review*, 48(3), 153–166. doi: [10.1109/emr.2020.3018420](https://doi.org/10.1109/emr.2020.3018420). Available from: <https://ieeexplore.ieee.org>

Further reading

- LiquiDonate (2023). How E-commerce businesses can mitigate return fraud and refund fraud. Available from: <https://liquidonate.com>
- McKinsey & Company (2023). Can E-commerce help customs agencies fix old problems?. Available from: <https://www.mckinsey.com>
- OECD (2023). Cross-border data flows. Available from: <https://www.oecd.org>
- United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) (2022). eDATA verifiable credentials for cross border trade. In *White Paper: United Nations Economic Commission for Europe*.

Corresponding author

Shiqiang Wang can be contacted at: wangshiqiang@cueb.edu.cn

For instructions on how to order reprints of this article, please visit our website:

www.emeraldgroupublishing.com/licensing/reprints.htm

Or contact us for further details: permissions@emeraldinsight.com