DOI: 10.54254/2754-1169/92/20231410

Challenges and Implications of AI in Digital Security

Yiwei Sun[1,a,*], Wenyunjin Zhang[2,b], Zexin Cai[3,c]

[1]Department of business, Xi'an University of Finance and Economics, SuZhou, 710100, China
[2]Department of Pre-U, Jurong Country Garden School, Zhenjiang, 212446, China
[3]Department of Pre-U, Jinan Foreign Language School, Jinan, 250031, China
a. 751433590@qq.com, b. 2903265583@qq.com, c. czx15688867010@163.com
**corresponding author*

Abstract: This article explores the challenges and implications of integrating artificial intelligence (AI) into digital security within the context of the rapidly evolving digital economy. It highlights the significance of data security in the digital age, particularly in cross-border data flows, and the need for effective policies to ensure safe and orderly data exchange. The study employs various methods, including technical evaluation of blockchain technology's potential in addressing data security challenges, and analyzes the impact of data protection standards on the European digital economy. The results emphasize the critical role of blockchain in decentralized data control, shedding light on the complexities of regulating data processors in a highly open and decentralized environment. The article also delves into the complexities of international cooperation in cross-border data regulation, suggesting the need for global international legal norms to harmonize data governance legislation. In conclusion, the article advocates for the integration of blockchain technology as a crucial component of a global cross-border data security system, offering technical innovation in tandem with legal frameworks. It underscores the importance of actively participating in the development of global data regulation standards to ensure data security in an interconnected digital world.

Keywords: cross-border data security, blockchain, decentralization, supervision, global data

1. Introduction

Artificial intelligence (AI), usually referred to as machine intelligence, is the intelligence displayed by machines that have been created by humans.Artificial intelligence is a term used to describe the technology that allows regular computer programs to mimic human intelligence.

Natural disasters are a manifestation of natural forces that cannot be countered by human beings alone, but if early warning can be done, many unnecessary casualties can be effectively reduced.With the advancement of technology, predicting natural disasters using artificial intelligence seems to be becoming a reality: Silvia Terra is a San Francisco-based company.The company uses artificial intelligence for forest mapping to provide resources for planners to help reduce the risk of fires; The team of China university, in collaboration with the China Seismic Administration, launched the world's first personal AI seismic monitoring system - "smart earthquake" monitoring systems [1], which can accurately estimate the parameters of the earthquakes source mechanism in one second, can also help predict the possible distribution of tsunami, strong surge. The accumulation of data in

© 2024 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

the face of one disaster and the storage of experience have reduced the number of natural disaster casualties from year to year.

The term "digital economy" was first introduced by American scholar Tapscott in his 1996 book "Digital Economy Age", which defined the "era" of the digital economy as an economic form for the application of information technology [2].The earliest explanation of the concept of a digital economy dates back to a government paper issued by the Ministry of Industry of Japan in May 1997, which clearly states that the basis of information technology, electronic means and an economy without physical mobility are characteristics of digital finance [3].The U.S. Department of Commerce's Emerging Digital Economy report, published in July 1998, states that e-commerce and the related technology industries that support e-business are an important component of the digital economy [4].It can be seen that early descriptions of the digital economy tended to be equated with e-commerce activities, concepts and definitions that may be limited to the application of Internet technology at the time.New communications technology and the accelerated integration of traditional economies make it even more difficult to define the concepts of the digital economy.

At present, the digital economy has become a strategic choice to seize the opportunity for a new round of technological revolution and industrial change.In the thirty-fourth collective study of the Political Bureau of the Central Committee of the Communist Party of China, General Secretary Xi Jinping emphasized that the rapid development of the digital economy, the broad range of radiation and the profoundness of shadow, are becoming a key force in the reorganization of global elements resources, re-shaping the global economic structure and changing global competition patterns.Unlike previous waves of economic globalization, China is no longer just a follower in the development of the digital economy, but plays a leading role in many areas.As a key productive element of the digital economy, data elements can play a magnifying, overlapping and multiplying role in socio-economic development only when they are fully available.Countries around the world attach great importance to data, a new type of national strategic asset, and the issue of cross-border data flow security has become the focus of the competitive game of the New Order.On a global scale, while cross-border data flows can greatly improve the efficiency of transnational collaboration, they also face difficulties in the coordination of conflicts of interest between economies, increased risks of cybersecurity and national security, and data sovereignty violations.

However, data security has been one of the critical issues that has been recognised.In the century of unprecedented change in the world, these data have not only effectively protected the safety of human life and property, but have also become a vital resource.The Global Times reporter was informed on 14th that a joint investigation team of the National Computer Virus Response Management Centre and 360 companies had made new progress in the cyberattack against the Wuhan City Emergency Administration's earthquake monitoring centre, finding backdoor malware that corresponded to the characteristics of the U.S. intelligence agencies.The next step will be to openly disclose to the outside world a highly classified global intelligence system of the United States Government, which poses a serious security threat to national security and world peace, both in our country and in the world.According to Chinese experts [5], the cyber attack by US intelligence agencies on the earthquake monitoring centre is a planned and premeditated cyber military reconnaissance operation that seeks to acquire the ability to analyze, investigate, attribute, position, etc. on our economic and even military operations, and may lead to social panic and chaos of order.Furthermore, it can be judged that cyber-attack intrusion and theft have become the least costly way for the United States to obtain remote sensing data from other countries.Meanwhile, the US side is also “crying for thieves,” claiming that “Chinese hackers are prepared to launch a destructive cyber attack on critical US infrastructure.”Experts reminded that in the face of the increasing trend of aggressiveness, initiative and aggression in the American concept of cyber space preparedness, there will be more and more cyber security confrontations initiated by the United States.Data security is all about us, from big to small countries to individuals.We do not want to prevent data exchanges or transactions, we just want them to be safe and lawful.

How to view AI challenges and impacts on data security in the context of the digital economy, and rational use of policies to promote the cross-border data safe and orderly flow and lead the development of digital economy globalization, are important topics to be studied in terms of data security. This paper first analyzes the impact of data security issues on economic globalization, then squeezes the constraints of cross-border data flow, and finally makes relevant policy recommendations in line with the data security status quo in China.

2. Methods

In researching the cross-border data security and its related issues, various materials and methods are available.

Method one, Technical Evaluation: Consider how blockchain technology is used in cross-border data flows, its viability and security, and its potential to address cross-border data security challenges.According to the study, cross-border data on blockchain has issues with the conventional two-layer regulatory structures.

Method two, Cooperation on a global scale: Examine how the digital economy in Europe will be impacted by European data protection standards.Analyze the effects of data flow obstacles on digital marketplaces, innovation, and enterprise development to better understand how its components influence data flow.

3. Result

The blockchain's core technology for decentralized data control (processing) offers the benefit of "decentralized" data processing while also bringing decentralization to the data processor itself [6]. This issue is particularly acute in a fully decentralized public chain where any individual or organization can send data, validate data, and take part in consensus. The traditional regulatory model for data processors faces a great challenge as a result of the "zero-threshold" openness of data processing, which has produced a large number of processors.

What’s more,this is because cross-border data control (processing) is a phased procedure that requires data entry, data intermediate processing, and data cross-border to be completed. In the data intermediary processing link [7], where a significant volume of data information is managed or processed by a non-local intermediate agency, there will inevitably be a lot of data transaction information [8]. As the foundation for its sanctions, the United States undertook data acquisition on the use of SWIFT controls and monitored worldwide data flows based on those data.cutting off the connection with SWIFT allows sanctioned States to block cross-border payments.That is, if cross-border data processors are not local institutions, the regulatory State's ability to oversee them is significantly diminished.

However, issues of international cooperation in cross-border data regulation based on blockchain.The global international rule of cross-border data regulation follows the basic logic of data regulatory jurisdiction for missing data.

The best way to resolve the rule-conflict between the parties in traditional cross-border data flows is to create a global international legal norm for data regulation based on harmonized data governance legislation between European countries [9]. This is because cross-jurisdictional data flows, which involve transboundary data flow, require numerous reviews and are in compliance with the data supervision rules of each jurisdiction.

Regional international legal standards are still geographically limited in the field of cross-border data transfers, but global international legal standards are broadly applicable. The United States has adopted the "prohibition of data localization" as a general principle [10], advocating that members should not prohibit or restrict the transboundary transfer of information (including personal information) by electronic means by businesses or individuals for commercial purposes, that data localization requirements should be prohibited, and that businesses and individuals should not be required to use computing facilities in their own country or to have access to certain data in order to transact business. The EU, on the other hand, adopted a more nuanced approach, contending that local data storage should not result in a trade distortion while simultaneously respecting the security standards of the nations involved in cross-border transmission.Data security is a top priority for data service providers in many developing nations because they lack the technological capacity to prevent and control cyberattacks and because there will be greater demands for data localization.Countries including India, Indonesia, and South Africa pushed for data localization and opposed cross-border data flows during the 2019 G20 Summit.

4. Discussion and Conclusion

In the context of the digital era, the rapid development of blockchain technology has accelerated technological innovation in the area of cross-border data information. At the same time, the global economy needs technical dynamism to integrate the digital economy with the traditional economy and the rule of law provides assurances. As the system for transboundary data flow changes, we should also actively investigate the use of blockchain technology for cross-border data security and establish a technological fortress for the global cross-bonded data security system. At the same time, we should promote and participate in creating global regulations for data supervision of blockchain transborder payments.

References

[1] *Uncle Van, 2021-04-18 18:04. The world's first artificial-intelligent earthquake surveillance system "Smart Earth Movement" arrives, can touch the earthquakes in one second https://baijiahao.baidu.com/s?id=1697357117680275368&wfr=spider&for=pc*

[2] *Tapscott,T.The digital economy: Promise and peril in the age of networked intelli gence[M]. New York: McGraw-Hill,1996.*

[3] *Wang Tong . Dialysis Day Electronics Business [EB/OL].(2000- 12-15)[2021-06-15],http://www.cnw.com.cn/issues/2000/15/1512.asp.*

[4] *Li Junjiang, He Xiaoyin. American Digital Economy Analysis [J]. Economics and Management Studies, 2005(07): 13-18.*

[5] *Feng Yaren, Ding Yazhi and Yuan Hong, 2023-08-15 06:31. The Chinese side locked the network into Wuhan earthquake monitoring center, expert: the attackers have obvious military reconnaissance purposes.*

[6] *R.V. Aguilera, K. Desender, M.K. Bednar, J.H. Lee Connecting the Dots: Bringing External Corporate Governance into the Corporate Governance Puzzle Academy of Management Annals, 9 (1) (2015), pp. 483-573*

[7] *Zheng X., Cai Z.Privacy-preserved data sharing towards multiple parties in industrial IoTsIEEE J. Sel. Areas Commun., 38 (5) (2020), pp. 968-979*

[8] *Wu Changyang, May 2022. Anti-monopoly regulatory study of data monopoly behavior,https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C475KOm_zrgu4lQARvep2SAkaWjBDt8_rTOnKA7PWSN5MAIp3EKsR0AjParARQratDZaVq78jgbAUumCyEQwzQ-I&uniplatform=NZKPT*

[9] *Jiao Huiping, 31 May 2023, Study on the Compliance of Transboundary Data Flow Regulations with International Economic and Trade Rules https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C475KOm_zrgu4sq25HxUBNNTmIbFx6y0bOQ0cH_CuEtpsDrUt8FeK2skrtAUYvRZbu1Q0UGt3TAvarzIpHQ7jaJF&uniplatform=NZKPT*

[10] *Gao Minhan, 2022-06-30. Study on legal regulations relating to the transboundary movement of personal data https://xuewen.cnki.net/CMFD-1022450654.nh.html*