ISSN 2616-7433 Vol. 6, Issue 1: 12-17, DOI: 10.25236/FSST.2024.060103

Study on the Rule of Law of Cyberspace Governance from the Perspective of Digital Guangxi

Huang Yuzheng

School of Law, Guilin University of Electronic Technology, Guilin, China
Hyz961014@163.com

Abstract: *As the engine of a new round of scientific and technological revolution, the importance of the Internet in human society has become increasingly prominent, accompanied by various problems in cyberspace governance, such as data security and data sovereignty issues, the positioning of public power subjects, the responsibility of big data platforms and algorithm problems. In the face of various problems, we must improve the legal system of data security, determine the reasonable boundary of public power, clarify the responsibility of big data platforms, and build a systematic algorithm regulation system. The introduction of the Guangxi Big Data Regulation provides a new paradigm for local legislation in cyberspace governance and escorts the construction of cyberspace governance system.*

Keywords: *Governance of cyberspace; The big data; Internet*

1. Introduction

With the new round of scientific and technological revolution and industrial transformation reshaping the global economy and society, cyberspace, as a new frontier for human innovation and development, has gradually become an important area of national and social governance in the new era, and the strategic significance of cyberspace governance has become increasingly prominent. In recent years, China's cyberspace governance has achieved remarkable results in the rule of law, the core technology in the information field has been continuously broken through, the network security protection system has been continuously improved, and the ecological governance of network information content has achieved effective results, but there are still many problems to be solved.

2. The problem of law in cyberspace governance

2.1. Data security and data sovereignty

National security cannot be separated from data. As a basic and strategic production factor resource of a country, data is closely related to the fate of the current country and nation. The virtual, global and interconnected nature of cyberspace determines that data sovereignty corresponding to the traditional physical space is inevitably in conflict, and the unique globalization of data itself also determines its cross-border flow and global sharing is inevitable. However, the difference in data development level caused by the unbalanced economic and technological development level among various countries and regions. It will inevitably lead to contradictions and conflicts between national data sovereignty and cross-border data flow. The reason: the ability to store, transfer, and process data may give some countries a political and technical first-mover advantage, leading to supranational data flows that may ultimately lead to a loss of national sovereignty. The traditional concept of sovereignty is also facing new challenges with the development of web3.0, which is characterized by virtuality and decentralization.

In addition, the cross-border flow of personal data may also create a series of risks such as data leakage and jurisdictional conflicts. The development of big data, cloud computing and other technologies has led to the backwardness of the "bottom-up" information security management method in cross-border data supervision in China. The imperfect rules of data classification and classification protection mode also constitute the main manifestation of contradictions in the field of data security in our country.

ISSN 2616-7433 Vol. 6, Issue 1: 12-17, DOI: 10.25236/FSST.2024.060103

2.2. The positioning of public power subjects in cyberspace

The offside and absence of public power in cyberspace are deeply affected by the legal relationship and value concept in cyberspace. With the prominent penetration of public law on private law in the Internet era and the influence of the traditional value concept of the supremacy of public power, criminal law, which should abide by the principle of restraint, is often off-side and takes the lead in the governance of chaos in cyberspace. The 2016 "QVOd case" is a vivid portrayal of this kind of tough interference of criminal paternalism in social governance. In our country's criminal justice for a long time, the value of the doctrine of heavy punishment makes the handling of the above cases controversial. Faced with the phenomenon of the offside of the public power subject in the rule of law governance of cyberspace under the promotion of criminal law activism, we should inquire into its legitimacy and rationality.

The opposite is the absence of public power in the rule of law of cyberspace governance. The absence of public power in cyberspace, which should provide social services and legal protection, is caused by three aspects: first, the lag of law. And this is due to the continuous leap of big data technology produced by various network chaos increased the technical pressure of legislation. Second, the traditional legal relationship is quietly changing in the Internet era, changing the traditional pattern of rights and obligations between the government, platforms and individuals.[1] The ambiguity of the boundary between public law and private law and the coexistence of various legal relations in cyberspace lead to conflicts in the application of existing laws. Third, in the jurisdiction of cyberspace, the virtuality and borderlessness of the Internet make the power of cyberspace governance prevaricate or compete, which intensifies the difficulty of cyberspace governance.

2.3. Responsibilities of big data platforms in data processing

The complexity of technology determines the role of big data platforms and the diversity of rights and obligations. Traditional accountability ideas are inadequate under the excuse of "technology neutrality". The existing data supervision accountability mechanism is unclear, the lag in the start of accountability, and the unreasonable distribution of responsibility, which makes it urgent to clarify the responsibility and identification mechanism of the platform data processors. Due to the "passive" supervision mode adopted by China for a long time, the accountability mechanism for data processors is often started after data leakage, and it is difficult to fundamentally solve the problem of data leakage. Low illegal cost, large data scale and low attention make data leakage easily occur in the process of cross-border data flow, which will pose a non-negligible risk to citizens' personal privacy and even national security.

As an important "intangible asset" in modern society, data supervision should not only be a passive post-remedial measure, but should be transformed into a pre-prevention link. Clarifying the responsibility boundary and accountability mechanism of data processors is a key link.

2.4. Algorithm regulation

The algorithm technology constitutes the whole underlying technical operation mechanism of the Internet platform, however, the algorithm also causes a series of risks. One is the problem of algorithm infringement. In the current era of traffic first, the core driving force for the survival and development of major Internet platforms is the various data of platform users. Driven by this business logic, users' personal privacy and data rights and interests will inevitably suffer damage. Typically, in the "Toutiao Infringement of Users' Personal Privacy Case" in 2019, Toutiao collected a large number of users' mobile phone content information, such as contacts, without explicitly informing the collection platform users' personal information in its app Privacy Agreement, causing a serious violation of users' privacy rights and contradicting the principle of "reasonable and necessary" information collection. The second is the problem of computational law training. Computational law training refers to the platform through the algorithm to use the massive data collected by the user to build a "user portrait", and then affect the user behavior. Foucault proposed in Discipline and Punishment that the panoptica prison realized the discipline of power on people, and the algorithm in the era of big data realized the new discipline on people.[2] In fact, this is the platform to build its "algorithmic hegemony", the algorithm makes users only contact the content they are interested in for a long time, which leads to users restricted in the "information cocoon", which will further create group polarization and deepen the knowledge gap.

ISSN 2616-7433 Vol. 6, Issue 1: 12-17, DOI: 10.25236/FSST.2024.060103

3. The path of the rule of law in cyberspace governance

3.1. Improving legislation to safeguard data rights and interests

First, improve the relevant provisions of emergency legislation. In this battle against the epidemic, the Law on the Prevention and Control of Infectious Diseases, the Law on Emergency Response, and the Regulations on Emergency Response to Public Health Emergencies have played a role. In the early stage of the outbreak and spread of COVID-19, faced with the shutdown of traditional social operating mechanisms, data collection and use played an important role in tracing the source and analyzing the transmission path. However, these separate laws and regulations still show insufficient protection of personal information and data rights and interests in the application process. Therefore, it is particularly important to perfect the relevant provisions of emergency legislation.

The second is to adopt the combination framework of public law regulation and private law protection. At present, the main path of personal information protection is public law and private law, while the relevant laws and regulations of data protection are relatively scattered. The Seventh Amendment to the Criminal Law stipulates the crimes and penalties for infringing citizens' personal information. The Personal Information Protection Law, introduced in 2021, is China's first systematically formulated law on the protection of personal information, promoting the free flow of personal information while protecting citizens' personal information. Due to the dual nature of data, both the data subject and the enterprise that generate the data have certain rights and interests in the data. Therefore, the boundary of the rights of natural persons to personal data cannot be extended without limitation because of the protection of the rights and interests of natural persons, thus impeding the flow, sharing and utilization of data. Nor can we disregard the right of data companies to collect, store and exploit personal data lawfully at their expense. Just as in the COVID-19 prevention and control process, the principle of non-disclosure should be observed when collecting personal information, and personal information should be protected by not collecting irrelevant or unnecessary data.[3] On the other hand, the protection of public interests requires the right to moderate derogation of personal data. Threats such as asymmetric data information between enterprise platforms, technology companies and consumers, algorithmic discrimination caused by data gap, and other threats cannot be fully protected by private law alone. It is necessary to adopt a diversified and balanced path combining public law regulation and private law protection to better protect data rights and promote data flow.

3.2. Determining reasonable boundaries of public power

In the current cyberspace governance, there is a phenomenon of public power "overstepping the boundary", such as the "Li Wenliang" incident. In such cases, it can be found that the operation mode of public power subjects in cyberspace governance needs to be improved, the supervision power of public power departments must be clearly defined and limited, abide by the proportionality principle of administrative law, and explore ways of flexible law enforcement. In order to realize the effect of cyberspace governance while effectively safeguarding the legitimate rights and interests of citizens.

In cyberspace governance, public power should follow the justification of purpose, that is, the intervention criterion of public power is that the network information content is indeed illegal content, rather than that the content may cause negative public opinion and affect social stability.

At the same time, as far as the supervision method of public power in cyberspace governance is concerned, there are also certain problems in the scale. For example, some apps are forced by public authorities to restrict rectification or take them off the shelves directly. In fact, public power subjects can choose both rigid and soft ways to govern cyberspace, and sometimes choose a slightly softer way to deal with them. For such problems, it can be improved from the following aspects: First, to solve the self-regulatory mechanism within the industry association, the relevant industry internal self-inspection and other regulatory mechanisms will be restricted from the early stage of APP listing, rather than after the listing of intervention. Second, in the choice of current regulatory methods, public authorities often use direct removal of shelves and other regulatory methods in a crude manner, which may not only cause economic losses to operators, but also to consumers, resulting in an imbalance between the administrative actions implemented by public power subjects and the regulatory purposes to be achieved.

ISSN 2616-7433 Vol. 6, Issue 1: 12-17, DOI: 10.25236/FSST.2024.060103

3.3. Clarify the responsibilities of big data platforms

Firstly, the platform should undertake appropriate filtering obligations during the content upload stage. Filtering out infringing works and bad content by means of algorithms and manual review is a specific requirement for the platform's duty of care. The platform can set keyword filtering technology and key frame filtering technology, and combine the early warning information of the National Copyright Administration and copyright owners to automatically screen uploaded works. Taking short video platforms as an example, they can also reduce a large number of video handling behaviors by setting a limit on the number of videos uploaded by users per day, and can also immediately remove infringing videos if they are found.[4] The platform should also communicate the platform's content review standards and precautions to users, and guide users to upload legal and legitimate content.

Secondly, in the content distribution stage, the platform should strengthen the review of key links, and establish a notification response mechanism. Distinguish and label different types of accounts and content to help the platform conduct more targeted review and management, so as to reduce the risk of large-scale dissemination of infringing works. The platform shall actively respond to and notify, take necessary measures to delete, block or disconnect the infringing works, and protect the legitimate rights and interests of copyright owners. The platform can establish a sound copyright protection system, quickly deal with infringing works, and improve the efficiency and accuracy of copyright protection.

Thirdly, in the processing phase. The platform shall make use of the linkage review mechanism to establish a comparison library of infringing content when dealing with infringing content to avoid repeated infringement. The stage of dealing with infringing content refers to the process of deleting and shielding the infringing works after the platform has received or found the infringing works. In this process, there may be the risk of the infringing works being re-uploaded or re-uploaded after modification. In the stage of dealing with infringing content, the platform shall exert the linkage review mechanism between the account and the content to ensure that the infringing content can be found and processed quickly. Through the infringement content comparison library, the uploaded new content can be quickly compared and reviewed, so as to prevent repeated infringement and improve the efficiency and accuracy of copyright protection.

3.4. Construct the algorithm regulation system

First, we will improve legal regulation. First of all, the introduction of special legislation to prevent the risk of platform application. On the basis of the "Network Security Law", the behavior of the algorithm platform in the protection of users' personal information and data processing is regulated. The specific legislation of the algorithm platform should at least cover the following: It should be based on the protection of user rights; It is necessary to establish the whole process supervision system such as access, operation and risk control of the algorithm platform; Specify a mechanism for the platform to apply risk, algorithm and data governance in an orderly manner; It is necessary to insist on positive guidance and moderate intervention.[5] The disorderly expansion of platform power not only impacts the traditional social structure but also damages the rights of users and intensifies the scope and depth of platform risks. In the future, the legislative center of the platform should focus on risk prevention, gradually shift to the subsequent data processing environment and strengthen the regulation of data processing behavior. It should not only pay attention to the governance of the platform information content ecology, but also pay attention to various complex and variable risks that may be caused by algorithms.

The second is to transform the regulatory system. The "New Generation of Artificial Intelligence Development Plan" issued by The State Council clearly proposes to establish a sound open and transparent artificial intelligence regulatory system, implement a two-tier regulatory structure with equal emphasis on design accountability and application supervision, and realize the whole-process supervision of artificial intelligence algorithm design, product development and application of results. It is mainly manifested in two aspects: the examination obligation of enterprises to algorithms and the supervision power of administrative organs to algorithms. The latter has been elaborated in the previous article, and the former is mainly discussed here. The network service platform should take the initiative to undertake the algorithm

ISSN 2616-7433 Vol. 6, Issue 1: 12-17, DOI: 10.25236/FSST.2024.060103

4. Analysis of Guangxi Big Data Regulation

4.1. The necessity and feasibility of the introduction of the Guangxi Big Data Development Regulation

The Guangxi Digital Economy Development Plan (2018-2025) (Revised in 2021) issued by the People's Government of the Autonomous Region in 2021 and the Implementation Opinions on Accelerating the Development of Digital Transformation and Deepening the Construction of Digital Guangxi issued in 2022 clearly regard cyberspace governance as an important content of the construction of Digital Guangxi. Cyberspace governance plays an important role in comprehensively promoting the digital transformation and development of Guangxi, comprehensively enabling the transformation and upgrading of Guangxi's economy and society, generating new industries, new business forms and new models, and strengthening the new engine of economic development.

The Regulations on Big Data Development of Guangxi Zhuang Autonomous Region will come into effect on January 1, 2023. The Ordinance consists of 78 articles in eight chapters, including general provisions, infrastructure, data resources, data markets, development and application, data security, legal liability and supplementary provisions. The regulation is Guangxi's first local regulation in the field of data. Guangxi follows relevant laws and administrative regulations, takes the practices of other provinces as reference, and takes the practice of Guangxi as support, and strives to use the rule of law to lead, promote and guarantee the development of big data.

4.2. The main problems to be solved by the Guangxi Big Data Regulation

The regulation gives the definition of public data sharing and points out that public data should be shared as the principle, and not shared as an exception. According to the sharing type, the public data can be divided into three types: unconditional sharing, conditional sharing and non-sharing. To make public data public, it must be clearly defined as property rights. The main purpose of public data disclosure is to make public data be effectively developed and used, and the collection of public data is also a reflection of public institutions to perform their duties, with the goal of providing better public services and public products for the public. However, as a special public good, government data can have new value through secondary processing. The Regulations on the Development of Big Data lack the issue of ownership confirmation after multiple transfers of public data, and do not address the potential conflicts between public welfare objectives and commercial interests after data disclosure, and the content of harmonizing these rights and obligations. The definition of data and the scope of sharing and opening in Guangxi's data legislation cannot be completely different from the "disclosure upon application" of government information disclosure.

4.3. Evaluation of Guangxi Big Data Regulation

The regulations focus on the development of big data, set up a special "infrastructure" chapter, from the big data infrastructure planning, government infrastructure, information infrastructure, integration infrastructure, rural big data infrastructure and other aspects and multi-dimensional provisions, to promote the data economy, digital government and other aspects of the legal foundation. At the same time, the regulations stimulate the development vitality from the cultivation of data elements market, from multiple angles of policy support and cohesion of development forces, and serve the high-quality economic and social development of Guangxi.

In order to balance development and security, when Guangxi formulated the Regulation, on the basis of fully implementing the relevant provisions of the Data Security Law and the Personal Information Protection Law, it clarified the responsibilities before and after data processing activities, strengthened the management of data processing activities, put forward the disposal requirements after data processing activities, and increased the security guarantee.

5. Conclusions

The issues facing cyberspace governance are complex. The introduction of the regulation is not only a positive and specific action for Guangxi to implement the national big data strategy, but also a realistic demand for promoting the high-quality economic and social development of Guangxi. It is of great significance to improve the rule of law level of big data development in Guangxi, promote the

ISSN 2616-7433 Vol. 6, Issue 1: 12-17, DOI: 10.25236/FSST.2024.060103

solution of systemic and industrial problems encountered in the development of big data in Guangxi, guide the healthy development of big data industry, and promote the high-quality economic and social development of Guangxi.

Acknowledgement

Project funding：Innovation Project of GUET Graduate Education "Study on the rule of law of Cyberspace governance from the perspective of Digital Guangxi—Take the Regulation on Big Data Development in Guangxi Zhuang Autonomous Region as an example"(2023YCXS143).

References

[1] Liu Quan.(2023).The Integration of Digitalization and rule of Law in the Construction of Digital Government . Contemporary Law, 37(06), 15-25.
[2] Zhi Zhenfeng, Liu Jiakun.(2023).The Chinese plan of Internet information content governance. Jiangxi Social Sciences, 43(11), 176-187.
[3] Tian Wei, Hu Xinfeng.(2022).Research on Innovative Construction of Social governance in the context of "Internet Plus" . Journal of Hebei Open University, 27(06), 55-58.
[4] Yu Yang, Shang Fujin.(2019).Internet-based campaign governance: New characteristics and operational logic: A Study based on the "Qinglang" special action. Journal of Public Administration, 20(03), 64-75+169.
[5] Zhou Jianqing, Zhang Shizheng.(2019).Evaluation and optimization of Cyberspace Content governance policies: Analysis based on PMC index model. Journal of Northeast University (Social Sciences Edition), 25(04), 70-80.