• Article •

Legal Boundary of Cyberspace: the Normative Construction of International Good Laws in the Field of Digital Governance and the Challenge to the Global Governance System

Mengxu, Wang[1,*]

[1] Law School, Hunan University of Technology, Zhuzhou, China

[*] Corresponding Authors: Mengxu Wang. Email: 1393206974@qq.com

Received: 10 July 2024 Accepted: 31 July 2024 Published: 30 August 2024

Abstract: With the advent of the digital age, the global society is undergoing unprecedented changes. Emerging technologies such as artificial intelligence, blockchain and the Internet of Things are rapidly emerging, bringing new opportunities and challenges to global governance. Good international laws play a key role in digital governance, helping to formulate unified legal standards and rules, promote international cooperation, and maintain global stability and order. At the same time, emerging technologies pose many challenges to the law, such as privacy protection, cyber security and intellectual property issues. In this context, strategies and recommendations are made to address these challenges, emphasizing the close interaction of law and technology to ensure the sustainable development of emerging technologies and the overall interests of the society. Through the in-depth analysis of international good laws in the field of digital governance and the coping strategies of legal challenges, it can provide beneficial thinking and contribution to the realization of comprehensive good governance and sustainable development of global digital governance.

Keywords: International Good Law; Digital Governance; Legal Challenges; Global Governance; Emerging Technologies

1. Theoretical Framework of International Good Law and Digital Governance

As an important legal and moral guide, international good law provides us with a framework for understanding and addressing the challenges of transnational digital governance when exploring the issues of global governance in the digital age. With the rapid development of digital technology and the increasing expansion of global information networks, the international community is facing unprecedented governance challenges. These challenges involve not only the technology itself, but also how to strike a balance between protecting personal privacy, maintaining cyber security, and promoting freedom of information.

1.1 The Basic Theory of International Good Law

International good law, as a legal and ethical system spanning countries and cultures, aims to provide common rules and norms for the international community. Its fundamental purpose is to promote global justice, peace and stability, and ensure that actions in international relations meet generally accepted ethical and legal standards. This legal system is not only composed of written legal provisions, but is also deeply rooted in the long-term values and practices formed by the international community.

The core principles of international good law include respect for sovereign equality, non-interference in internal affairs, peaceful settlement of disputes, and respect for human rights and fundamental freedoms. These principles are not only the cornerstone of international law, but also an important criterion for guiding international relations and decision-making. For example, the principle of sovereign equality emphasizes the equal status of all countries before international law, while the principle of non-interference in internal affairs requires respect for the political independence and territorial integrity of each country. At the same time, the principle of peaceful settlement of disputes encourages states to resolve their differences through dialogue and negotiation, rather than through force or confrontation.

In the field of digital governance, these principles apply equally well. With the development of digital technology, international good laws need to adapt to new challenges, such as network security, data protection, and freedom of information. These emerging issues call for the development of new norms and standards to address the special needs of the digital age, while respecting the existing principles of good international law. Therefore, the application of international good law in the field of digital governance, not only need to follow its traditional principles, but also needs to modern interpret and expand these principles to ensure the effectiveness and fairness in the global digital environment.

1.2 The Basic Theory of International Good Law

Digital governance refers to the general term of the policies, rules and implementation process of coordinating the digital management mode and rules of various countries, promoting the reasonable circulation of data resources, and realizing the realization of data privacy protection and security management. The advent of the digital era has also had a profound impact on the law of the operation of international relations, and has marked the evolution of international norms with a deep digital brand. The current state of digital governance is reflected in the deep global dependence on digital technologies and cyberspace, and the growing influence of these technologies in the social, economic and political fields. With the spread of the Internet and the development of digital technology, information and data have become the key resources for driving innovation, promoting economic growth and shaping public policy. In this process, digital platforms have become an important place for information exchange, business transactions, and social interaction. However, this rapid technological evolution and global networking simultaneously pose many challenges.

The first is about data protection and privacy rights. The massive collection and processing of personal data, especially in commercial and government surveillance, has raised widespread concerns about privacy protection and data security. Differences in the laws and norms of data protection between countries and regions have further increased the complexity, leading to legal challenges in cross-border data flows. Second is the issue of network security. With the frequent occurrence of cyber attacks and data leakage incidents, cyber security has become the focus of global attention. Countries, enterprises and individuals all face cyber threats from different sources, which not only involve economic losses, but may also threaten national security and social stability. Moreover, freedom of information and censorship tension are also an important challenge. Globally, there is an intense debate about the free flow of information and the balance between national security, cultural values, and social morality. Different political and cultural backgrounds lead to different practices in network content management, which partly affects the free flow of information around the world. Finally, with the global connectivity brought about by digitization, the need for transnational legal coordination and cooperation is becoming increasingly urgent. How to establish an effective international legal framework and cooperation mechanism to deal with cross-border digital issues is a problem that needs the joint efforts of the international community.

All in all, the current state of digital governance reflects a rapidly growing, highly interconnected world, full of opportunities and challenges. In a fairly long period of time, it will be an international consensus for global digital governance to reach the international rules generally accepted by all parties and form a digital trade system for effective governance. In this diverse and complex environment, global cooperation, legal innovation, and policy adjustments are needed to address these challenges and take full advantage of the benefits of digitization.

1.3 The Intersection of International Good Law and Digital Governance

When we explore the intersection of international law and digital governance, we are actually considering two areas of interaction: the one the system of international legal and ethical principles, and the other the growing digital world and the complex governance challenges it poses. This intersection is particularly evident in several key areas. The intersection of international good law and digital governance is actually a dynamic and interactive field, in which international good law provides the basic framework and moral guide for dealing with complex problems in the digital age. Through continuous adaptation and innovation, international good law can play a positive and guiding role in the process of global digitization.

First, with the rapid development of information technology and the popularization of global networks, the international good law faces the problem of how to adapt to and guide the code of conduct in the digital space. For example, privacy protection, data security, intellectual property rights, and cross-border data flows are all issues that must be considered by good international law in the digital age. Here, international good law not only provides a legal framework, but also provides moral and

ethical guidance to help form a more just and transparent digital environment. Second, international laws play a key role in pushing the international community to reach consensus on digital governance. In the context of globalization, different countries have different legal systems and governance models, and international good laws have become a bridge to promote the dialogue and coordination between these different systems. Through international treaties, agreements, and other multilateral mechanisms, international good laws provide common reference standards and solutions for addressing transnational digital governance issues. Finally, the international good law shows its importance in dealing with the new legal issues caused by the rapid development of digital technology. With the rise of artificial intelligence, big data, blockchain and other technologies, the traditional legal framework is under the pressure to update and adapt. In this case, international good laws not only need to respond to the challenges of these emerging technologies, but also need to foresee the future development trends and form flexible and forward-looking legal norms.

2. Legal Challenges in the Global Digital Space

With the rapid development of digital technology and the deepening of global informatization, the global digital space has become a key part of modern society. This space not only facilitates global communications, business transactions, social interaction and knowledge sharing, but also raises a series of unprecedented legal challenges. The major legal issues presented in the global digital space include data protection and privacy, network security and freedom of information, as well as cross-border data flow and legal conflict. These challenges not only test the effectiveness and adaptability of the existing legal framework, but also put forward an urgent need for the further development of international good law.

2.1 Data Protection and Privacy Rights

In the global legal challenges in the digital space, data protection and privacy issues are particularly prominent. In a data-driven world, the collection, use, and transmission of personal data has become the norm in daily life. However, it has also raised concerns about personal privacy violations. As technology advances, our personal information is widely collected and analysed, from social media to online shopping to smart devices. This not only involves the security of personal information, but also concerns how to effectively protect this information in different legal fields.

The international attention to data protection and privacy rights has caused a series of legal and policy changes. For example, the European Union's General Data Protection Regulation (GDPR) marks an important milestone in data protection legislation, which sets strict rules for the processing of personal data and gives more control to individuals. However, differences in data protection laws between countries and regions contribute to the complexity of global governance in this area. For example, the US takes a more flexible approach in some ways than the strict EU regulations. These differences not only pose a series of compliance challenges in the operation of multinational companies, but also challenge the uniformity and coordination of international good laws in data protection.

Therefore, one of the major challenges to overcome in the global governance of data protection and privacy is how to coordinate the differences between different legal systems and develop a set of international standards that can both protect personal privacy and facilitate international data flow. This requires the concerted efforts of the international community to establish a more unified and efficient global data protection framework through dialogue and cooperation.

2.2 Network Security and Freedom of Information

In the global digital space, cyber security and freedom of information constitute a pair of complex and closely linked issues. On the one hand, with the acceleration of the digitization process, cyber security has become an important global concern. It involves protecting data from unauthorized access and destruction, ensuring the stability and security of network systems, and guarding against all types of cyber crimes and cyber terrorism. This is not only a technical issue, but also a major challenge for law and policy makers. In response to these threats, many countries and international organizations have formulated a series of cyber security laws, regulations and standards. However, these measures may also sometimes conflict with the guarantee of freedom of information. On the other hand, freedom of information, including freedom of speech and freedom of access to information, is the cornerstone of building an open and democratic society. In the digital age, this freedom plays a crucial role in promoting knowledge-sharing, supporting civic participation, and enhancing government transparency. However, the freedom of information in the network environment also faces challenges, arising from the censorship of network content, network monitoring, and legal restrictions on network expression.

Therefore, in the global digital space, there is a delicate balance between maintaining cyber security and safeguarding the freedom of information. Excessive security measures may infringe on personal privacy and restrict freedom of speech, while unrestricted freedom of information may threaten network security and social stability. The challenge of international law in this field lies in how to formulate and implement an effective legal framework that can effectively respond to cyber security threats and protect and promote freedom of information. This calls for in-depth dialogue and cooperation between policy makers, legal experts and technical experts around the world to explore solutions that fit the characteristics of the digital age.

2.3 Cross-Country Data Flows and Legal Conflict

Cross-country data flow and legal conflict is one of the most complex and challenging legal issues in the global digital space. As globalization and digitization accelerate, large amounts of personal and business data are transmitted across national borders, which not only drives economic growth and innovation, but also poses many legal and regulatory challenges. First, the legal differences in data protection and privacy rights between countries and regions lead to significant legal conflicts. For example, the EU's General Data Protection Regulation (GDPR) sets strict rules on data processing and cross-border data transmission, in sharp contrast to the relatively relaxed data protection laws in the United States. Therefore, when processing cross-border data, multinational companies may be subject

to the legal constraints of multiple jurisdictions at the same time, resulting in a significant increase in compliance costs and facing legal risks. Second, the regulation of transnational data flows is not only about privacy and business interests, but also about national security and sovereignty issues. Many countries restrict cross-border flows of data for national security reasons, which in turn affects the freedom of global data flow. For example, some countries require domestic data centers, or impose export restrictions on certain types of data. Moreover, the international community faces enormous challenges in the legal coordination of transnational data flows. While there are some international agreements and frameworks that attempt to harmonize data protection standards on a global scale, these efforts are often limited by differences in national interests, political will, and legal systems, so establishing a global unified data governance framework remains a distant goal. Therefore, cross-border data flow and legal conflict is a very challenging area in global digital governance, which requires not only the coordination of laws and policies among countries, but also balances the multiple needs of privacy protection, commercial interests and national security while respecting national sovereignty.

3. The Application and Practice of International Good Law in Digital Governance

In today's rapidly evolving digital age, the application and practice of international good law in digital governance has become an important field of global legal research. This area covers many key aspects, from data protection to network security to freedom of information, which are receiving unprecedented attention at a global level. With the continuous innovation and popularization of digital technology, the international community is faced with unprecedented legal challenges, which require that international law not only adapt to the pace of technological development, but also protect individual rights, safeguard international security, and promote legal and policy coordination among different countries. Therefore, an in-depth discussion of the application and practice of international good law in digital governance is not only crucial to understand the evolution of the modern legal framework, but also the key to understand and solve the complex problems faced in global digital governance.

3.1 The EU GDPR Case Analysis

The EU's General Data Protection Regulation (GDPR) represents an important milestone in international law in the digital age. As a revolutionary data protection regulation, GDPR reshapes the way personal data is processed, emphasizes the rights of data subjects, and sets completely new global standards for personal privacy. One of the core principles of the regulation is the privacy self-determination, which gives individuals full control over their personal data. GDPR also introduced concepts of data minimization, data portability and "right to be forgotten", which are now key components of global data governance. The global influence of GDPR is reflected in its extraterritorial effectiveness. Even non-EU businesses and organizations must comply with the GDPR rules as long as they process the personal data of EU residents. This has led to legal and policy changes worldwide, prompting many countries and regions to review and revise their data protection regulations to align

with the GDPR. In this way, GDPR not only implements a unified standard for data protection within the European Union, but also promotes the importance of digital privacy and data governance around the world. However, the implementation of GDPR has also brought a series of challenges and controversies, especially when it is aligned with the data protection standards in other countries. The compliance costs that companies bear to comply with the GDPR, the complexity of processing cross-border data transmission, and the differences in data regulation with countries such as the United States all demonstrate the complexity and challenge of the application of international law in digital governance.

1. International Influence Analysis of GDPR

Since the implementation of the General Data Protection Regulation (GDPR), its influence on global data protection and privacy standards is evident. The GDPR marks a new and more rigorous approach to personal data protection, influencing business practice and legal policy worldwide. First, it caused a global return to data privacy and protection, with many non-EU countries began to revise or develop their own data protection laws to approach or meet the GDPR criteria. For example, Japan, Brazil, Canada and other countries have updated their data protection laws. Second, the extraterritorial effectiveness of the GDPR means that any company in the world processing EU residents' data, wherever it is located, must comply with these rules. This has forced international companies to reassess their data processing and privacy policies, and even their entire business model. Moreover, GDPR affects rules for international trade and data flow, especially in cross-border data transmission.

2. Relationship between GDPR and International Good Law

International agreements play a crucial role in cybersecurity governance, not only because of the remarkable transnational nature of cybersecurity issues, but also because the resolution of these problems requires cooperation and coordination on a global scale. In the digital age, the rapid development of information technology and the global nature of cyberspace make it difficult for a single country to cope up to cyber threats and challenges independently. Therefore, international agreements play a key role in setting global cyber security standards, promoting information sharing, strengthening transnational cooperation and building a common cyber defense system.

Through international agreements, countries can jointly determine the norms of conduct in cyberspace, including but not limited to determining the definition of cyber attacks, stipulating legal cyber behavior, and setting standards for data protection and privacy rights. For example, the European Union's Network Information Security Directive (NIS Directive) is aimed at strengthening cooperation among member states on the protection of critical network infrastructures. In addition, the United Nations and other international organizations are also promoting cooperation on global cyber security issues, strengthening international cooperation through the formulation of international guiding principles and initiatives to respond to increasingly complex cyber security threats. International agreements also promote the sharing of technology and intelligence, which is crucial to improving countries' ability to prevent, detect and respond to cyber attacks. Through information sharing, countries

can more effectively identify and respond to cyber security threats, including cyber crime, cyber espionage, and cyber warfare. Furthermore, these agreements also help to coordinate national laws and policies to ensure consistent legal action and sanctions against cybercrime on a global scale.

However, the implementation of international protocols in cybersecurity governance also faces challenges. Differences in cyber security concepts, legal system and technical capabilities between different countries may lead to implementation difficulty and resistance to cooperation. Therefore, although international agreements are crucial for global cyber security governance, their effectiveness is largely dependent on the willingness and implementation of countries. In short, international agreements play an indispensable role in building a more secure, coordinated and unified global cyberspace. In the future, as cybersecurity challenges evolve, these protocols need to be constantly updated and refined to adapt to new security threats and technological changes.

From a regional perspective, the internationalization of China's banking industry shows the characteristics of taking Hong Kong as a springboard, supporting by Asia and radiating to other parts of the world.

China's Hong Kong Special Administrative Region is often the first stop for overseas development of Chinese banks. In the last century, Hong Kong branches of the four major state-owned banks or controlled Hong Kong banks have played an important role in Hong Kong's banking industry. In particular, BOC Hong Kong was once a note-issuing bank in Hong Kong. This special status reflects the important position of Chinese banks in Hong Kong's banking industry. Furthermore, not only the four major state-owned banks, but also joint-stock banks such as Shanghai Pudong Development Bank and China Merchants Bank have set up branches or subsidiaries in Hong Kong, taking the first step of their internationalization.

Based on Hong Kong, China's banking industry will often further expand into the Asian market. Among the overseas branches of state-owned banks in China, the number of branches located in Asia is relatively large. On the one hand, because the number of Asian countries accounts for a relatively high proportion in the national number, it will inevitably lead to more branches in Asia, on the other hand, it shows that Chinese banks attach great importance to the Asian market. There are two main reasons for this phenomenon. First, because Asian countries are close to China in location, have cultural similarities, and are relatively friendly to China in politics, it is more favorable for Chinese banks to do business here. Secondly, it is also guided by the policies of the China government. In recent years, the government of China has repeatedly advocated the construction of the Belt and Road Economic Circle, and most Asian countries are located in the economic circle, so it has naturally become an ideal area for Chinese banks to develop.

Moreover, Chinese banks have established more institutions in Europe and North America. This phenomenon is also easily understood. New York, London, Frankfurt, etc. are all internationally renowned financial centers, and Chinese banks can better carry out all kinds of business by setting up branches here. At the same time, there are a large number of overseas Chinese in these countries, and

the establishment of branches by Chinese banks in these areas has also played a political role in serving local Chinese.

It is obvious that Chinese banks have fewer branches in Africa and Latin America. This is related to the development of local economy and financial industry. However, with the increasing exchanges between China and Africa, Chinese banks are gradually exploring the African market.

3.2 Network Security and Freedom of Information

In the global digital space, cyber security and freedom of information constitute a pair of complex and closely linked issues. On the one hand, with the acceleration of the digitization process, cyber security has become an important global concern. It involves protecting data from unauthorized access and destruction, ensuring the stability and security of network systems, and guarding against all types of cyber crimes and cyber terrorism. This is not only a technical issue, but also a major challenge for law and policy makers. In response to these threats, many countries and international organizations have formulated a series of cyber security laws, regulations and standards. However, these measures may also sometimes conflict with the guarantee of freedom of information. On the other hand, freedom of information, including freedom of speech and freedom of access to information, is the cornerstone of building an open and democratic society. In the digital age, this freedom plays a crucial role in promoting knowledge-sharing, supporting civic participation, and enhancing government transparency. However, the freedom of information in the network environment also faces challenges, arising from the censorship of network content, network monitoring, and legal restrictions on network expression.

Therefore, in the global digital space, there is a delicate balance between maintaining cyber security and safeguarding the freedom of information. Excessive security measures may infringe on personal privacy and restrict freedom of speech, while unrestricted freedom of information may threaten network security and social stability. The challenge of international law in this field lies in how to formulate and implement an effective legal framework that can effectively respond to cyber security threats and protect and promote freedom of information. This calls for in-depth dialogue and cooperation between policy makers, legal experts and technical experts around the world to explore solutions that fit the characteristics of the digital age.

3.3 Cross-Country Data Flows and Legal Conflict

International organizations play a vital role in digital governance, which is particularly evident in the context of the rapid development of globalization and digitization. First, international organizations, such as the United Nations, the International Telecommunication Union (ITU), and the World Trade Organization (WTO), provide a platform for dialogue and cooperation between countries on the formulation of digital policies and standards. Through these platforms, countries can discuss and address key issues in the digital age, such as cross-border data flows, cyber security, and e-commerce. Such international cooperation is crucial to formulating unified digital governance norms, as the nature of

digital technology and cyberspace crosses national borders, and the policies and regulations of a single country are often difficult to effectively respond to global challenges and opportunities.

In addition, international organizations play an important role in promoting knowledge-sharing and technology transfer. They organize various international conferences and seminars that provide professional training and technical support to help developing countries improve their digital governance capabilities. For example, UNESCO (UNESCO) has carried out a series of projects in the areas of digital cultural heritage protection and freedom of access to information. International organizations also play a key role in standard setting and the promotion of best practices. By publishing guidelines and standards, international organizations help countries understand and implement effective digital governance strategies, which are essential to ensuring the security and stability of the global cyberspace. For example, the International Telecommunication Union has issued a series of guidance documents related to network security and ICT standards.

However, the role of international organizations in digital governance also faces challenges. Differences in digital policies and governance ideas between different countries sometimes lead to slow progress in international consultation and cooperation. In addition, the rapid development of technology also brings challenges to the formulation of long-term and effective international standards and policies. Overall, international organizations play an indispensable role in building a safe, inclusive and sustainable global digital governance system. They not only provide a platform for multilateral dialogue and cooperation, but also play an important role in knowledge sharing, technology transfer, and standard setting. Despite the challenges, they still have a significant impact in driving progress in the field of global digital governance.

4. Legal Adaptability and Innovation in the Global Governance System

Under the tide of the digital age, the traditional legal framework is facing unprecedented challenges. With the change of the world political and economic situation, the traditional global governance mechanism has been impacted, the new digital governance rules have not been established, and the institutional supply is seriously missing. Globalization and the rapid development of technology have not only reshaped the way of international communication, but also put forward new requirements for the existing legal system. We need to analyze in depth how, in this dynamic and rapidly changing environment, the global governance system meets the emerging challenges through legal adaptability and innovation.

4.1 The Interaction between Law and Technology

Educational accountability in the era of digital governance depends more on the comprehensive application of educational data, but there are often uncertainties in the cross-border transformation of technology, and convenience and efficiency are hidden data ethical risks. The interaction between law and technology is a complex and continuous development process. This interaction requires the law to constantly adapt to the new technological environment, while ensuring that technological development

meets the ethical and legal standards of society. To achieve this goal, ongoing dialogue and cooperation are needed among lawmakers, technical experts and society. As the maintainer of social norms and order, law is faced with the challenge of constant adaptation and updating under the background of the rapid development of technology. With the emergence of new technologies, such as artificial intelligence, big data, blockchain, and the Internet of Things, the legal system needs to be updated in a timely manner to solve the new problems and challenges posed by these technologies. For example, privacy protection laws need to be adjusted in response to the massive collection and processing of personal data, while intellectual property laws need to adapt to new forms of digital innovation.

At the same time, the development of technology is also influenced by the existing laws and norms. Law not only provides the legal framework for technology development, but also affects the application mode and direction of technology. For example, data protection laws affect how companies collect and use data, while cybersecurity laws determine how companies protect themselves from cyberattacks. Moreover, the law also exerts influence on technological development in terms of moral and social values, ensuring that technological innovation is consistent with the overall interests of society. In the interaction between law and technology, some special phenomena appear. On the one hand, legislation often lags behind the speed of technological development, which causes the so-called "legal lag phenomenon". Lawmakers are challenged to anticipate and understand trends in new technologies, and they also need to develop effective norms without hindering innovation. On the other hand, the continuous development of technology also provides new tools and methods for law implementation, such as the use of big data and algorithms to enhance the efficiency of law enforcement, or the use of blockchain technology to ensure the transparency and security of contracts.

4.2 International Legal Coordination and Cooperation

In today's globalized world, countries are increasingly closely connected in terms of economy, society, science and technology, which makes international legal coordination the key to maintaining the global order and promoting international cooperation. With the development of digitalization, cyberspace security is facing more complex and severe challenges, and many issues need to start with cross-border cooperation. International legal coordination involves mutual adjustment and consultation between different legal systems of different countries, aiming to achieve common legal standards and rules in order to better handle cross-border issues such as international trade, environmental protection, human rights protection, cyber security and so on. Despite the challenges, a more just, effective and comprehensive international legal system can be gradually constructed through the joint efforts of all countries.

However, international legal coordination faces many challenges. First, different countries have significant differences in their legal systems, political systems, cultural backgrounds, and economic development levels, which complicate reaching consensus and uniform standards. Secondly, international legal coordination must also take into account the complexity of national sovereignty and

international relations to ensure that international legal rules do not violate the sovereign rights of all countries. Moreover, global issues of inequality and injustices, such as economic and technological disparities between developed and developing countries, also bring additional difficulty in legal coordination. In this context, international cooperation is particularly important. Through international organizations, multilateral agreements and international conferences, countries can jointly discuss, formulate and implement the rules of international law. Such cooperation will not only help to overcome the difficulties in international coordination, but also provide a platform for a joint response to global challenges. For example, international cooperation has achieved some results in such areas as climate change, human rights protection, and international trade.

4.3 Emerging Technologies to legal challenges

The rapid development of emerging technologies, such as artificial intelligence, blockchain and quantum computing, are constantly changing our way of society and life. However, these new technologies also bring a series of complex legal challenges, involving privacy protection, intellectual property rights, ethics and many other fields. To address these challenges, the legal community faces important tasks for innovative legal strategies to ensure the rational application of emerging technologies and protect the public interest and social values.

When it comes to the strategies of emerging technologies to address legal challenges, the following key aspects need to be explored in more detail: 1. Regular legal review and update: Lawmakers need to establish mechanisms to regularly review existing laws to ensure that they keep pace with the development of emerging technologies. This can be achieved by establishing a dedicated technical legal review body or committee, whose mandate is to monitor technical trends, propose legal amendments, and ensure the continued adaptability of the law.2. Technical impact assessment: Technical impact assessment should be conducted when formulating new regulations or revising existing laws. This includes analyzing the potential impact that new technologies may have on the social, economic and legal systems in order to better understand the need for legal adjustment. This can be achieved through the cooperation of the legal and technical experts.3. Multistakeholder participation: When formulating laws and policies, the voices of all stakeholders, including technology companies, consumer groups, non-governmental organizations and academia. This multi-party engagement helps to ensure that legal strategies are more comprehensive and balanced to meet the needs of different interests.4. Adoption of international standards: Given the global characteristics of emerging technologies, the adoption of international standards is crucial. Lawmakers should actively participate in the development process of international standards to ensure that their domestic laws are consistent with international standards. This helps to promote international cooperation and cross-border technology interoperability.5. Technical training of law: Legal practitioners need to receive training related to new technologies to better understand technical issues and provide professional legal advice. This helps to bridge the knowledge gap between the legal and technical fields and make the law more targeted and practical.6.

Regulate tech companies: Large tech companies in emerging technologies tend to have huge market power and data collection capabilities. Lawmakers need to consider how these companies to ensure that their actions do not abuse technology and violate user rights. This could include creating antitrust rules and data privacy regulations.7. Development of ethical framework: Due to different values, countries will emphasize different priorities in digital governance. For some emerging technologies, such as AI and gene editing, an ethical framework should be developed to guide their development and gene application. This helps to ensure that the development of technology coincides with social ethical values and preventing potential abuse and risks.

To sum up, addressing the legal challenges posed by emerging technologies requires a range of comprehensive strategies, covering legal update, technology impact assessment, multi-party participation, international cooperation, training of legal practitioners, regulatory and ethical framework of technology companies. The effective implementation of these strategies will help to ensure that the law can remain effective and beneficial in the tide of technological development.

5. Conclusion

Good international law plays an important role in the field of digital governance, helping to formulate unified legal standards and rules, promote international cooperation, and maintain global stability and order. However, the rapid development of emerging technologies also brings many challenges to the law and needs continuous research and discussion. At the acceleration of global entry into a digital society, the number of conflicts or different interests in the digital sector is obviously increasing. It requires international organizations and multilateral mechanisms to achieve governance outcomes that include both formal rules and standards as well as various informal institutional arrangements. This study highlights the interaction between law and technology, and the importance of international legal coordination and cooperation, providing strategies and suggestions for addressing legal challenges. Through a comprehensive analysis of these issues, this paper aims to provide insights into understanding and promoting the application and development of international good law in the digital age, so as to promote the effectiveness and impartiality of global digital governance. Although this paper discusses the key issues of international good law in digital governance, there is still a lot of room for discussion. We hope to further in-depth research and discussion to promote the comprehensive good governance and sustainable development of global digital governance. In the digital age, the harmonious development of law and technology will be an important issue facing the global society, which requires joint efforts.

Acknowledgement

None.

Funding Statement

None.

Author Contributions

The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

Availability of Data and Materials

None.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1]. Gao Wanglai.(2021).Artificial intelligence and digital governance in the post-epidemic era [J]. The Contemporary World and Socialism, (06): 25-33.

[2]. Zhang Plateau. (2023).The new situation of global digital governance in the era of great power strategic competition and China's response plan [J]. Leadership Science, (01): 21-25.

[3]. Yi Ming, Zheng Jiaqi, Lu Conni.(2023). Digital trade international rules under the perspective of global digital governance [J]. Foreign economic and trade practice, (04): 10-14.

[4]. Yao Lu, He Jiali.(2021).The multiple roles of global digital governance in national security [J]. Modern International Relations, (09): 28-35 + 53 + 61.

[5]. And Gao Wenxin, Yue Hu.(2023).Data-driven, Evidence-based Improvement and Responsibility Sharing: International Experience and Local Inspiration for Educational Accountability in the Era of Digital Governance [J]. Contemporary Education and Culture,15 (03): 55-62.

[6]. Huang Lihong. (2019).Research on the Reform of China's Digital Silk Road and Global Governance in the Digital Era [J]. E-government, (10): 56-67.

[7]. Zhang Monan.(2021).Global Digital Governance: Disagreements, Challenges and China Countermeasures [J]. Open Guide, (06): 31-37.