

Research on Information Security Protection in The Context of Post-epidemic Tourism Revival

Anqi Mei, Xinru Tang, Wenlong Wei, Yifei Niu

Jiangsu Police College, Nanjing 210000, China

Abstract: After the epidemic, the tourism industry is experiencing an unprecedented revival, and the problem of information security has gradually become an important factor restricting the development of tourism. Through in-depth analysis of the background of tourism revival, the challenges faced and domestic and foreign laws and regulations and other issues, this paper puts forward a series of targeted solutions, including investment in technical construction, provide infrastructure and other technical means, as well as improve the relevant laws and regulations, establish and improve the enterprise management mechanism and strengthen supervision and other non-technical strategies. These measures help to ensure the data security of the tourism industry in the process of digital transformation, and promote the healthy and sustainable development of the tourism industry.

Keywords: Post-epidemic tourism; Information security; Laws and regulations.

1. Introduction

The global epidemic is gradually under control, and the tourism sector is gradually showing vitality. However, in the process of tourism recovery after the epidemic, information security protection has become an important issue. With the rapid development of information technology and the digital transformation of the tourism industry, the tourism industry is facing more and more information security challenges, such as data leakage, network attacks, malware and so on. These security issues not only have a direct impact on the operation of the tourism industry, but may also endanger the privacy and security of tourists. Therefore, it is of great theoretical and practical significance to study the information security protection in the context of post-epidemic tourism revival, so as to formulate corresponding countermeasures and measures. This paper aims to discuss the issue of information security protection and put forward corresponding suggestions against the background of post-epidemic tourism revival. Meanwhile, it is also hoped that under the background of tourism revival, all sectors of society will pay attention to information security protection and jointly promote the sustainable development and safe operation of tourism. Through the development of this study, we can provide theoretical support and practical guidance for related research fields and promote the development of tourism information security protection.

2. Background of Post-epidemic Tourism Revival

Due to the impact of public health emergencies and the need for prevention and control, the movement of people around the world has been restricted, the scale of tourism has shrunk sharply, and the tourism industry has ushered in the winter season. To cope with the difficulties, some enterprises have begun to seek online business models, attracting tourists through online live broadcasting and virtual Tours. This exploration has a certain positive effect on reducing the adverse impact of the epidemic on business operations and promoting the informatization construction of the tourism industry, but it may also lead to problems such as forced

consumption and personal information leakage.

3. Analysis of Challenges and Causes of Tourism Information Security

With the impact of the epidemic and the development of science and technology such as the Internet, big data and artificial intelligence, in the process of recovering the tourism market, short-distance travel has become a realistic choice for Chinese tourists after the epidemic. After the outbreak, although people are enthusiastic about traveling, they are still cautious about traveling. As can be seen from Ctrip's report on the popular tourist destinations of the May Day holiday in 2020, the number of consumers who choose short trips is more, such as driving by train to travel nearby, and the recovery of long-distance trips that need to take planes is slower.^[1]The role of "cloud tourism" in promoting the marketing and promotion of scenic spots has become increasingly prominent. Biometric technology has been more widely used in the tourism industry. The continuous growth of the number of tourists has led to the appointment system becoming the norm. However, the problem of information security has become a major challenge affecting the sustainable and healthy development of tourism. To correctly understand and deal with the potential risks and challenges of post-epidemic tourism information security is one of the keys to further promote the high-quality development of tourism. "According to Tongcheng Travel's previously released financial report, its revenue in the second quarter of 2023 reached 2.87 billion yuan, an increase of 117.4 percent year-on-year. Adjusted net profit was 590 million yuan, up 428.9 percent year on year. The average monthly active users reached 280 million, up 53.5 percent from the same period in 2019; And 42.2 million average monthly paying users, up 52.3% from the same period in 2019. The company's core performance indicators, including revenue, adjusted net profit and average monthly paying users, all hit record highs."^[2]While the tourism industry is recovering rapidly, the development of the tourism industry affected by the big environment has also shown obvious changes compared with that before the epidemic.

At present, China's data protection regulations are not perfect, and there are no specific legal provisions for the information security protection of the tourism industry, which may lead to security problems such as data leakage, abuse or tampering. And the process of tourism hotel check-in, ticket reservation and other links involve a large number of customer data, including identity information, payment information and other sensitive data, once these data is leaked, may lead to a series of problems, such as fraud, identity theft. This not only poses a threat to personal privacy, but may also cause damage to the reputation and business of tourism companies. However, due to the lack of tourism information data regulations, law enforcement departments may encounter difficulties in enforcement. For example, it is difficult to determine which actions violate regulations, or to impose effective penalties for violations. Therefore, tourism enterprises lack effective legal support and basis when carrying out information security protection, and are prone to data management confusion and irregular law enforcement procedures in practice.; At the same time, the lack of information security talents in the tourism industry is a common problem. With the digital transformation of the travel industry, the risk of cyber attacks also increases, and hackers may use various ways to hack into the systems of travel companies, steal customer information, disrupt business operations, and even blackmail companies. However, some tourism enterprises may not have a professional information security team, or some tourism management departments and enterprises have insufficient investment in the training of information security protection, resulting in the lack of corresponding professional knowledge and skills of talents, resulting in the insufficient ability of information security teams to cope with increasingly complex cyber attacks and information security issues; In addition, the lack of emergency response mechanism is another important reason for tourism information security protection. Some tourism enterprises have not established a perfect emergency response mechanism, or the implementation of the emergency response mechanism is insufficient, resulting in the inability to respond to network attacks and information security incidents in a timely manner. The lack of effective means of information collection and analysis will also affect the accuracy and timeliness of emergency decision-making; After the epidemic, the tourism industry is still facing industry reshuffle. Whether enterprises can adapt to a series of changes in consumption concepts and whether they can transform into sustainable operations are all challenges faced by information security protection.

4. Domestic and Foreign Information Security Protection Policies and Regulations

4.1. Legislative Level

With the rapid development of information technology, there are more and more ways to obtain personal information, and the risk of personal information exposure also increases. The legislation on information security protection inside and outside the region has been constantly improved.

In recent years, China has issued a series of information security protection policies and laws and regulations. For example, the Cybersecurity Law of the People's Republic of China provides an important guarantee for promoting the healthy development of economic and social informatization

and ensuring the healthy operation of the Internet on the track of rule of law. The Law of the People's Republic of China on the Protection of Personal Information is of great significance in ensuring the security of citizens' personal privacy. At the same time, in order to regulate the collection and storage of data, ensure the security of the use of personal information, and protect the legitimate rights and interests of individuals and organizations, the Data Security Law of the People's Republic of China, which was officially implemented on September 1, 2021, provides a legal basis for the reasonable and lawful application of big data. In addition, Article 52 of China's Tourism Law also makes clear requirements for tourism operators, requiring them to keep tourists' personal information confidential during business activities. In addition to constantly improving the legislation, in order to better protect the security of citizens' personal information, China has also formulated relevant implementation rules and normative documents, such as the "Network Security review Measures" and "Data Security Management Measures", to further promote the application of big data in the field of digital economy.

From the perspective of legislation, both domestic and foreign countries attach importance to the protection of tourism information security and have formulated a series of laws, regulations and related policies to ensure the security of tourists' personal information, regulate the collection and use of tourists' personal information by tourism-related institutions and enterprises, and provide a legal basis for combating related criminal activities. However, although China has been making efforts in the protection of personal information security, compared with foreign countries, it is still far from enough. From the perspective of development history, foreign countries have carried out legislative activities in the aspect of personal information security protection as early as the last century. In the 1970s, the United States promulgated the Privacy Act on privacy protection. The Personal Information Protection and Electronic Documents Act (PIPEDA), which came into effect in Canada in January 2001, clearly stipulates the standards and requirements for the protection of personal information, including the collection and use of data. From the perspective of legislative level and effectiveness, China's legislation on information security protection is mainly formulated by the executive department, while the European Union and the United States and other national information security protection policies and regulations are mainly formulated by national institutions such as the Congress or parliament, whose legislative level is higher and has higher effectiveness; From the perspective of content, most of the specific contents stipulated by relevant domestic laws and regulations or policies are only for domestic tourism, while relevant foreign laws also emphasize the regulation and management of transnational tourism, for example, the General Data Protection Regulation (GDPR) passed by the European Union in May 2018 requires multinational enterprises to comply with the relevant provisions of GDPR. Otherwise, multinational enterprises will face huge fines or legal proceedings. In addition, domestic regulations on information security protection mainly focus on issues of personal information protection and network security management, and the division of responsibilities of Internet participants is not clear enough. In contrast to foreign practices, the information security protection policies and regulations of countries such as the EU and the United States are more

detailed, including not only personal information protection issues, but also national security, cyber crime and other fields, and the division of responsibilities of Internet participants is also more detailed.

From the content of these laws and regulations and the time of promulgation and implementation, it is not difficult to see that there is still a certain gap between China and some foreign developed countries in terms of personal privacy protection and data collection and use, which still needs continuous research and learning.

4.2. Administrative Level

Domestic tourism information still faces many challenges in terms of administration. On the one hand, the laws and regulations on tourism information security are not perfect, which leads to insufficient supervision and can not effectively protect the security of tourism information. On the other hand, the government's supervision of the tourism market still needs to be strengthened, especially in dealing with emergencies and protecting the rights and interests of tourists.

Compared with the domestic situation, the development of tourism information administration in foreign countries shows different characteristics. In many developed countries, the tourism information administration system has been quite mature. By establishing perfect tourism information service platforms, these countries provide rich and accurate tourism information and provide quality services for tourists. At the same time, the government departments have relatively strong supervision over the tourism market, which ensures the healthy development of the tourism market. Of course, there are also challenges in the administrative aspects of foreign tourism information. With the continuous expansion and complexity of the global tourism market, how to deal with various emergencies and protect the rights and interests of tourists has become a major problem. In addition, how to provide quality services while protecting tourists' privacy is also a problem waiting to be solved. First, the scope and procedures for the collection, use and disclosure of tourist information by government agencies and public service departments should be clearly stipulated in administrative law to ensure that tourist information will not be abused. Second, supervision and accountability over the collection, use and disclosure of tourist information by government agencies and public service departments should be strengthened in administrative law to prevent abuse of power. Finally, government agencies and public service departments should be encouraged to adopt technological innovations to improve the level of tourist information protection.

4.3. Judicial Level

In the post-epidemic context, information security protection in domestic and foreign tourism has become an important issue. In specific judicial cases, such as the data breaches at Marriott Hotels and Carnival Corporation, these cases highlight the risks and responsibilities of travel companies when handling tourists' personal information. To prevent similar incidents, travel companies are required to establish an internal control mechanism for personal information protection in data compliance and raise the awareness of cyber security among practitioners.

From the perspective of comparative law, the importance of personal information protection has been emphasized in the judicial practice of tourism information security protection after the epidemic at home and abroad, but there are

differences in specific measures and legal environments. China's approach focuses more on regulating the behavior of the tourism industry through legal notices and guidance documents, emphasizing the synergy between administrative organs and judicial organs. While foreign countries, especially European countries, focus more on protecting information security through legislation and international agreements, while focusing on the security management of the entire value chain of the tourism industry; In terms of the impact of the epidemic on tourism information security protection, both countries are facing the challenge of how to protect tourists' personal information from abuse while safeguarding public health. While China manages tourists' information through measures such as real-name system and health code, foreign countries may achieve this through more detailed health and security protocols. In general, the judicial practice of tourism information security protection at home and abroad is constantly developing and improving, aiming to find a balance between protecting personal privacy and promoting tourism recovery. China's practice is more reflected in the guidance of laws and policies, while foreign countries may focus more on international cooperation and the formulation of agreements. In the future, with the gradual recovery of the tourism industry, both are likely to continue to strengthen laws and regulations on information security protection to adapt to the new tourism market environment.

5. Countermeasures of Post-epidemic Tourism Information Security Protection

After the epidemic, the tourism market has been revitalized. While the economic benefits brought by tourism have increased and people's aspirations have been met, many problems have also arisen, which require the joint efforts of the state, society, enterprises and individuals.

First of all, from the perspective of legislation, the improvement of laws and regulations is the most basic and effective guarantee for the development of tourism. Regulations and regulations can greatly restrain businesses and lawbreakers who steal information for profit. Therefore, according to the characteristics and needs of tourism, it is necessary to formulate laws and regulations specifically for tourism information security, clarify the responsibilities and obligations of tourism information security, regulate the behavior of tourism enterprises, and strengthen the protection and management of tourism information. Improve relevant laws and regulations for the protection of personal data, increase penalties for personal data breaches, and increase the cost of illegal activities; Formulate relevant laws and regulations on data security and network security, regulate the behavior of enterprises and individuals, and prevent the occurrence of security incidents such as data leakage and network attacks.

Second, the strengthening of investment in technology construction and the improvement of related infrastructure need to be implemented as soon as possible. With the rapid development of electronic tourism, making travel plans, purchasing tickets and tickets, booking hotels and so on through the Internet has gradually become the norm. The electronization of tourism has realized the goal of participating in various travel reservation activities by means of convenient and low-cost network transactions, greatly improving efficiency and reducing costs. Tourism electronic

technology is based on computer technology, so in order to better protect tourism information security, it is necessary to strengthen the construction of technology such as firewall technology, encryption technology and identity authentication. At the same time, the infrastructure of tourism information service includes both hardware and software. The software includes the construction of tourism website, information center and trading platform, and the hardware includes the establishment of tourism consulting department and the issuance of brochures. The improvement and consolidation of infrastructure can effectively avoid the generation of poor information, make it easier for tourists to identify false information and enjoy tourism services more conveniently^[3].

Thirdly, enterprises should consolidate the internal supervision and management mechanism, strictly abide by laws and regulations, and improve the ability of enterprises to protect consumers' personal information. Enterprises should cultivate employees' keen sense of information security issues and strengthen information security management, formulate internal rules and regulations, clarify the responsibilities and obligations of information security, regulate the behavior of employees, establish personal information protection systems, adopt encryption, access control and other measures to ensure the security of personal information^[4]; In addition, the enterprise should also establish an emergency response mechanism, for the occurrence of information security incidents, can take timely measures to reduce losses to the greatest extent. At the same time, enterprises need to regularly increase emergency drills to improve their ability to cope with emergencies. In addition, some tourism management departments and enterprises should pay attention to the training of talents in the field of information security, increase the investment of resources and energy in the building of information security teams, build professional teams, and improve the ability to protect tourists' information security.

Finally, it is important to strengthen the supervision of the tourism industry^[5]. Establish a sound supervision mechanism, including daily inspection, special inspection, complaint handling, etc., this mechanism can find and deal with the information security problems in the tourism industry in a timely manner; Since the information security of the tourism industry involves many departments, such as tourism, public security, communication management, etc., therefore, it is necessary to strengthen the cooperation between departments to jointly deal with the information security problems in the tourism industry. The relevant government departments should also publicize the information security knowledge to the tourist audience, and remind them to protect their personal information.

In addition, a large number of existing practices at home and abroad have proved that strengthening law enforcement and international cooperation, establishing an information sharing mechanism, and strengthening technology research and development and application are important countermeasures for information security protection after the epidemic. Some countries have strengthened law enforcement against the tourism industry and cracked down on violations of information security regulations. Taking Southeast Asian countries as an example, Myanmar and Cambodia are strengthening cooperation with China in the tourism industry, providing tourism services and security, and attracting Chinese tourists, while also stepping up the fight against criminal activities. In addition, Europe will roll out new

health and safety protocols for all links of the tourism value chain to create a safer travel environment. International organisations such as the World Tourism Organisation are also pushing for a safe relaunch, highlighting the importance of speeding up vaccination and supporting tourism; Some countries have established information sharing mechanisms to enhance cooperation and information exchange between governments and enterprises. The United States, Japan, Germany, Spain, Hong Kong and other countries and regions have established business cooperation and information sharing mechanisms through joint legislation, which has promoted information sharing and collaboration between governments and enterprises, and improved the defense capability of information security; Some countries have strengthened technology research and development and application, adopted advanced information security technologies and products, and improved the information security protection capabilities of tourism enterprises. For example, in March 2023, the Organization for Economic Cooperation and Development (OECD), an intergovernmental organization for international economic cooperation comprising 30 market economy countries, released a document entitled "Emerging Privacy-Enhancing Technologies - Current Regulatory and Policy Approaches Report", which reviews recent technological advances in the area of privacy enhancement, and assesses the different types of technological maturity and the opportunities and challenges that come with it. These technologies encrypt, back up and verify travel data, ensuring the security and integrity of the data.

In the context of the revival of tourism, there is still a long way to go in information security protection, given the importance of information security protection and its imperfect protection mechanism. As the tourism industry moves towards digitalization, the public will pay more attention to information security. In order to protect the information security of the tourism industry, major tourism enterprises and government departments need to strengthen information security awareness education, develop and improve information security management systems, improve information security capabilities, and ensure the normal development of the tourism industry. At present, the government and enterprises are taking active measures to ensure the security of tourism users' information and interests. In the future, there will certainly be more advanced technology and more complete management mode to protect information security. It is also necessary to have more assistance from corresponding technical talents and improve the personal quality of tourism employees. To sum up, tourism rejuvenation and information security protection complement each other. Only on the premise of ensuring information security can the tourism industry develop smoothly and vigorously, so as to provide people with better, safer and more assured travel experience.

Acknowledgment

Project Fund: Research Project on Information Security Protection in the Context of Post-Epidemic Tourism Revival under the Training Program of Practical Innovation and Entrepreneurship for College Students of Jiangsu Province, Project number: 202310329036Y.

References

- [1] See the 2020 Labor Day travel new trends forecast, Trip.com; Ctrip's 2019 Labor Day travel trends forecast, Trip.com.
- [2] Wang Xiaoyu, Huang Xingli. Tourism rebounds strongly! Ctrip's revenue exceeds pre-epidemic [N]. China Times, 2023-09-11(012).
- [3] Jiang Li. Network Information Security Technology in Tourism E-commerce [J]. Neijiang Science and Technology, 2009, 30(03): 117-118.
- [4] Xu Chang. Research on Information Security Problems and Countermeasures in the process of Tourism Enterprise Informatization Construction [J]. Electronic world, 2016, (20) : 33 + 32-35 DOI: 10.19353 / j.carol carroll nki DZSJ. 20161103.001.
- [5] Wan Yanxia. Research on the construction of Guilin Tourism safety information Public service system [D]. Guangxi Normal University, 2014.