SEIZING THE OPPORTUNITIES OF GOOD GOVERNANCE UNDER THE RULE OF LAW, AND ENJOYING THE ACHIEVEMENTS OF THE DIGITAL DEVELOPMENT: CTRIP'S BUSINESS PRACTICES IN DATA SECURITY AND PRIVACY PROTECTION

Wang Xin

TABLE OF CONTENTS

SEIZING THE OPPORTUNITIES OF GOOD GOVERNANCE UNDER THE RULE OF LAW, AND ENJOYING THE ACHIEVEMENTS OF THE DIGITAL DEVELOPMENT: CTRIP'S BUSINESS PRACTICES IN DATA SECURITY AND PRIVACY PROTECTION

Wang Xin[*]

Ctrip was founded in Shanghai in 1999. Thanks to the rapid development of China's Internet and the continuous improvement in cyberspace rule of law, Ctrip has seized the opportunity to thrive in the online travel industry and has been constantly developing in a standardized manner. In recent years, with revolutionary innovations in the field of artificial intelligence and the high-quality development of cyberspace rule of law that provides strong protection, Ctrip and other Internet enterprises have been able to fully focus on breaking through new technologies, planning new scenarios, providing new services, and achieving new developments. We have reflected on personal information and data systems.

I. THE CONTINUOUS IMPROVEMENT OF PERSONAL INFORMATION AND DATA SYSTEMS IS CRUCIAL FOR THE HIGH-QUALITY DEVELOPMENT OF THE DIGITAL ECONOMY AND THE SUSTAINABLE DEVELOPMENT OF INTERNET PLATFORMS

As the core element of the digital economy, data derive value from the ability to flow and integrate across different entities. However, with the development, circulation, and utilization of data, their value has become increasingly prominent, while security risks such as data breaches and theft have grown, seriously impacting the stability of digital economic activities. Currently, the digital economy is accelerating its integration with the real economy with various types of data growing rapidly and accumulating in large quantities. The position of data as a fundamental and strategic production factor is becoming increasingly prominent. At the same time, this has raised new and higher demands for data governance capabilities.

* Vice President of Ctrip Group.

China has formulated and promulgated more than 150 pieces of legislation in the field of cyberspace, especially laws such as the *Cybersecurity Law*, *Data Security Law*, and *Personal Information Protection Law*, which provide fundamental guidelines for Internet platforms to handle users' personal information and ensure data protection. The promulgation of measures and regulations has further refined the requirements for personal information and data protection. For example, the *Interim Measures for the Management of Generative Artificial Intelligence Services* implement inclusive and cautious, as well as category-based and tiered, regulation for generative AI services, clearly defining the requirements for different stages such as training data processing, data annotation, and service provision, and encouraging the innovative development of generative AI. The *Regulations on the Management of Network Data Security* further specify the provisions for personal information protection, which set out the overall requirements and general provisions for network data security management, improving systems for securing important data, optimizing regulations on cross-border network data security, and clarifying the obligations of network platform service providers, thereby maintaining fair market competition. These measures are beneficial for protecting the legitimate rights and interests of individuals and enterprises in cyberspace, ensuring economic development and national security, and further promoting the high-quality and sustainable development of China's digital economy.

II. STRENGTHENING THE INTERNAL CONSTRUCTION OF PERSONAL INFORMATION AND DATA SYSTEMS ON PLATFORMS, AND ACTIVELY IMPLEMENTING RESPONSIBILITIES FOR THE PERSONAL INFORMATION AND NETWORK DATA SECURITY MANAGEMENT

Internet platforms are leaders in the application of technology in the era of artificial intelligence, hubs of digital activities, and aggregation areas for data resources. As a one-stop online travel service platform that serves over 100 million travel bookings annually across 220 countries and regions, Ctrip's development is closely intertwined with data and information

governance. From the company's perspective, data are the cornerstone and prerequisite for the stable operation of global business and serve as resources and assets for the innovation of travel products and services. From the perspective of consumers, data are essential for the fulfillment of online services and represent full trust in the platform's security. From the perspective of partners, data is the bridge and link for supply chain cooperation. Any delay, interruption, or breach of data affects the user experience and sustainable development of the company. Ctrip attaches great importance to data security and privacy protection and treats them as the core for building resilience and security in the online travel industry chain. The company has implemented over a hundred measures across eight major areas: organizational management, rule and system establishment, technical control, audit and supervision, certification and training, rights protection, emergency response, and data sharing.

In terms of organizational management, a leadership team has been established, headed by the Chief Technology Officer and consisting of heads from information security and various business lines, to coordinate and oversee the group's data security and privacy protection efforts. Under the leadership team, working groups have been established with departments such as information security, legal affairs, and government affairs to implement specific work requirements. In addition, task-specific teams were formed as needed. For instance, to strengthen personal information protection, the company's senior leadership directs and coordinates the establishment of a special coordination group for personal information protection.

In terms of the rule and system establishment, based on the *Cybersecurity Law*, *Data Security Law*, *Personal Information Protection Law*, and other regulatory standards and requirements, an internal management system has been established, covering data security, personal information protection, mobile app compliance, and more. This system is dynamically updated in accordance with the laws and regulations, regulatory directives, and user feedback. At the same time, a working mechanism has been established in which business and compliance departments share responsibilities. Any newly released app version must first pass internal security testing before it can be launched online, ensuring full process coverage of needs assessment,

product design, secure development, data collection, data transmission, data usage, and data destruction.

In terms of the technical control, industry-leading security technologies and services such as access control, dynamic authorization, key management, behavior pattern baseline analysis, security watermarking, encryption for storage and transmission, expiration-based destruction or anonymization, degaussing machines and professional third-party disk destruction are comprehensively applied to achieve the minimum collection, minimum access and minimum use of personal information and data.

In terms of audit and supervision, multiple measures are taken, including personnel position management, behavioral event management, and internal and external audit management. All personnel engaged in personal information and data processing positions are required to sign confidentiality agreements and undergo background checks. Security audit functions are enabled for network devices, security equipment, application systems, and other assets. The audit covers items such as traffic logs, daily operations, system maintenance, data destruction records, and major security incidents, with audit records collected and stored in real-time and regularly backed up. Internal and external audit inspections are conducted periodically, including interviews, on-site checks, and specialized tool inspections, with supervision and rectification efforts promoted accordingly.

In terms of certification and training, the company has successively obtained security certifications such as ISO 27001, ISO 27701, and PCI-DSS. Every year, online information security training and examinations are conducted for all employees, covering topics such as personal information laws and regulations, app privacy, data sharing, data cross-border transfer, and anti-phishing protection. Additionally, specialized personal information and data security training are provided for personnel in data processing roles, including product and development staff, customer service, and data analysts.

In terms of rights protection, users' rights to know and to choose are fully guaranteed. The privacy policy clearly and comprehensively discloses the ways in which users can exercise their rights to query, correct, supplement, manage, delete, and cancel their personal information. Any change in usage scenarios or data collection will be communicated to users through updated

privacy policies, pop-up windows, or other methods to obtain their consent. Customer service personnel immediately notify the information security team for complaints related to personal information and data protection, which then collaborates with business and legal teams to resolve the issue within the specified time frame. Additionally, contact information for the Reporting Center for Illegal and Harmful Information under the Cyberspace Administration of China and consumer complaints is provided.

In terms of emergency response, a classified and tiered emergency response system for security incidents has been established along with an emergency response team. The responsibilities of various parties, including information security, IT, legal affairs, and government affairs, have been clearly defined. Additionally, emergency response plans have been formulated and corresponding annual drills are conducted.

In terms of data sharing, personal information and other data are shared only with necessary partners. Background checks are conducted on partner personnel and qualifications, information security audits and risk assessments. Meanwhile, confidentiality agreements and data processing agreements are signed, covering security requirements, such as data protection, data transmission and storage, and access control. When sharing data through SDKs, third-party SDKs can only be embedded into the Ctrip app after passing a security assessment, and the privacy policy clearly informs the users of the SDK providers, its purpose, the fields of information collected, and links to the privacy policy.

Currently, Ctrip's platform handles the outbound transfer of personal information and data related to flight bookings, hotels, and vacation reservations. As a specific scenario and subset of data security and privacy protection, Ctrip applies the same or even higher security standards for the outbound transfer of personal information and data as those used domestically in compliance with national laws, technical standards, and regulatory directives.

Thanks to the country's cautious and inclusive regulatory policies, Ctrip's outbound transfer of personal information and data falls under exceptional scenario of 'where personal information has to be transferred outside China for the purpose of entering into or performing contracts to which the individual is a contracting party' stipulated in the *Regulations*

on Promoting and Regulating the Cross-Border Data Flow, and is exempt from the outbound data transfer security assessment, personal information outbound transfer standard contract and personal information protection certification. This significantly reduces the company's compliance and cross-border service trade costs, effectively supporting its international expansion and the dual circulation development of both domestic and global markets.

Although Ctrip has conducted in-depth and detailed explorations and business practices in the field of data security and privacy protection, it also faces new problems and challenges brought about by the 'data explosion' in the age of artificial intelligence. For example, consumer deepfake fraud triggered by AI technologies such as face-swapping and voice-changing, AI-driven hacker attacks, large model data annotation, anti-tampering and ethical security, and AI-generated false information. These emerging issues pose risks of transmission and amplification in complex cross-border service environments and new Internet spaces such as the metaverse. Moreover, we face divergent value orientations, priorities, and methodologies in the global governance of artificial intelligence and big data across different countries, as well as objective barriers to standard certification interoperability and mutual recognition. These challenges will greatly test the policy wisdom of regulatory authorities and compliance of enterprises. Therefore, we look forward to exploring feasible approaches and best practice cases that balance development and security under the guidance and assistance of relevant authorities, addressing common industry issues and unique business challenges, and fostering a better global trade environment to seize global development opportunities.

(Translated by Liu Yan)
(Edited by Li Jiesi)