NEWSLETTER
LIFANG & PARTNERS 立方观评
关注更多精彩内容
No.224
2021.04

Weekly Cybersecurity and Data Protection Review No.49

By Lifang & Partners

Domestic News

The Standing Committee of the Anhui Provincial People's Congress Passes the Regulations on Big Data Development in Anhui Province

The Supreme People's Court Issues Opinions on Providing Judicial Services and Guarantees for the Construction of the "Two Zones" in Beijing

CCA Comments on Restaurants' Mandatory "Scan Code Ordering"

Shenzhen Seeks Advice on the Regulations on the Management of Intelligent and Connected Vehicle

CAC: Step up to Formulate the Data Security Law and Personal Information nProtection Law

China Citic Bank Fined CNY 4.5 Million for Leaking Customer Account Information

Overseas News

EU and U.S. Intensify Negotiations on Transatlantic Data Privacy Flows

Parliament of India Issues Report on The Consumer Protection Rules, 2020

Roskomnadzor Proposes Expansion of Personal Data Law to Include Foreign Internet Entities

Day Before Election, 6.5 Million Israel's Voters Data Leaked Online

Ikea France Being Prosecuted for Spying on Staff

Domestic News

The Standing Committee of the Anhui Provincial People's Congress Passes the Regulations on Big Data Development in Anhui Province

On March 26, 2021, the Standing Committee of the Anhui Provincial People's Congress voted and passed the *Regulations on Big Data Development in Anhui Province*. In order to strengthen data security protection, the *Regulations* clearly implements a data security responsibility system. Cybersecurity department, public security department and telecommunications management department along with other related departments are responsible for the security protection work of big data, whereas the relevant departments of the people's government at or above the county level for strengthening their monitoring, early warning, controlling and emergency reponse capabilities of anti-attack, anti-breach and anti-theft in the context of big data. The *Regulations* also requires all departments to perform data security management responsibilities and strengthen social data security education. (More)

The Supreme People's Court Issues Opinions on Providing Judicial Services and Guarantees for the Construction of the "Two Zones" in Beijing

On March 26, 2021, the Supreme People's Court issued the *Opinions on the People's Court Providing Judicial Services and Guarantees for the Construction of Beijing's Integrated National Demonstration Zone for Opening-up the Service Sector and the China (Beijing) Pilot Free Trade Zone*. According to the *Opinions*, the people's courts should serve the development of new business models of the digital economy, properly handle cases in the new business fields such as online education, online medical care, telecommuting and online exhibitions, pay close attention to the new types of cases arising from the co-development of big data and other fields such as transportation, cultural tourism, catering services and modern manufacturing, promote the industrial upgrading, protect the legal rights and interests of consumers and promote the data economy and entity economy to integrate deeply. The people's courts should also strengthen the judicial protection of new digital infrastructure constructions such as 5G, big-data platforms and Internet of Vehicles, of digital empowerment and transformation of traditional infrastructures, and of construction of digital economy demonstration application scenarios, facilitating to build an internationally competitive digital industry cluster in Beijing, and turning Beijing to become a benchmark city of global digital economy. (More)

CCA Comments on Restaurants' Mandatory "Scan Code Ordering"

On March 25, 2021, the China Consumers Association ("**CCA**") expressed its opinions on reastaurants compelling consumers to scan code to order food. The CCA believes that the restaurants' mandatory "scan code ordering", which collects consumers' mobile phone numbers, birthday, geographical locations and other information unrelated to catering consumption violates the "Lawfulness, Fairness and Necessity Principle" of collecting and using personal information, and is suspected for over-collecting consumers' personal information. Meanwhile, this behavior fails to consider the capabilities of the vulnerable (such as the elderly and minors) to use smart phones, and objectively creates obstacles for their consumption. Moreover, the vulnerable are less aware of risk prevention and therefore more likely to become victims of personal information breach and payment security issues. The application of new technology should not become an excuse to over-collect consumers' personal information, nor should it become a barrier to public consumption. (More)

Shenzhen Seeks Advice on the Regulations on the Management of Intelligent and Connected Vehicle

On March 23, 2021, the Standing Committee of the Shenzhen Municipal People's Congress seeks advice from the society on the *Regulations on the Management of Intelligent and Connected Vehicle*. Chapter 5 of the *Regulations* stipulates rules on cybersecurity and data protection. Among them, regarding data opening, Article 33 of the *Regulations* stipulates that after applying to and being approved by the traffic and transportation management department of the public security authority, the intelligent and connected vehicle operating companies can obtain desensitized data information related to their intelligent and connected vehicle products such as road violations and traffic accidents. In terms of data protection, Article 34 of the *Regulations* stipulates that companies related to intelligent and connected vehicle should take precautions, to prevent personal information breach, loss, and damage, and formulate plans for data security and privacy protection. When the information breach, loss, and damage of national security data and users' personal information happen or may happen, relevant companies should take remedial measures immediately, promply notify the users and report to the municipal cybersecurity department. Meanwhile, the *Regulations* also prohibits illegal collecting, processing, and using of personal privacy and information, and prohibits illegal collection of data regarding national security. (More)

CAC: Step up to Formulate the Data Security Law and Personal Information nProtection Law

On March 19, 2021, Yang Xiaowei, deputy director of the Cyberspace Administration of China ("**CAC**"), attended a press conference held by the State Council Information Office and answered reporters' questions on improving data security and privacy protection capabilities. He said that in order to continue strengthening data security and personal privacy protection under the background of rapid development of big data, CAC will step up to formulate the *Data Security Law* and the *Personal Information Protection Law*, which will provide judicial guarantees for data security and personal privacy protection. CAC will also continuously strengthen the protection capabilities of national critical information infrastructure; strengthen the early warning and tracing of data security issue; speed up the formulation of relevant regulations and standards; establish relevant systems for the confirmation, opening, circulation, and transaction of data resources; improve the protection system of data property rights; strengthen law enforcement of data security and personal information; and strengthen the data security education. (More)

China Citic Bank Fined CNY 4.5 Million for Leaking Customer Account Information

On March 19, 2021, the China Citic Bank was punished by the China Banking and Insurance Regulatory Commission ("**CBIRC**") for leaking customer information. Previously, a talk show actor reported to the CBIRC, claiming that without his authorization and legal investigation procedures by judicial authorities, China Citic Bank directly provided his bank account transaction details to his former employer. After investigation, CBIRC found that China Citic Bank has compliance issues such as implementation of imperfect customer information protection system and mechanism, improper management of customer information collection process, incomprehensive control and management of customer data access, poor protection of customer sensitive information and loopholes in system authority management. China Citic Bank was fined CNY 4.5 million. (More)

Overseas News

EU and U.S. Intensify Negotiations on Transatlantic Data Privacy Flows

On March 25, 2021, EU Commissioner for Justice, Didier Reynders, and U.S. Secretary of Commerce, Gina Raimondo, made the following statement regarding the negotiations on transatlantic data privacy flows: "The U.S. Government and the European Commission have decided to intensify negotiations on an enhanced EU-U.S. Privacy Shield framework to comply with the July 16, 2020 judgment of the Court of Justice of the European Union in the Schrems II case." The EU-U.S. Privacy Shield was a mechanism for transfers of personal data from EU companies to companies in the U.S. that adhered to the mechanism. It was in place since 2016. On July 16, 2020, the European Court of Justice invalidated the EU-U.S. Privacy Shield. (More)

Parliament of India Issues Report on The Consumer Protection Rules, 2020

On March 24, 2021, Parliament of India issued the report on the Consumer Protection (E-Commerce) Rules, 2020. The report introduced the risks that E-Commerce consumers are exposed to and the various types of threats they could encounter at each level of his/her online shopping process. For example, when ordering products, consumers are taking the risks that their behavior pattern data being misused and they being exposed to malicious recommender system algorithm. When paying online, the consumers might encounter phishing and salami attacks. The Committee, therefore, recommends that user's personal data may be categorized as per their level of sensitivity and appropriate protection level may be assigned for each level. The Committee further recommends that the Ministry of Consumer Affairs should ensure that a secured and robust system of payment gateway is made available to the Consumers so that the transaction related data of the users is not compromised in any way. Further, the Committee felt that all major e-marketplace entities should establish their data centre in India, so that the Consumer data are not hosted in a server located beyond the borders of the Country, which may be misused by an enemy Country. (More)

Roskomnadzor Proposes Expansion of Personal Data Law to Include Foreign Internet Entities

On March 23, 2021, according to *Data Guidance*, the Russian Federal Service for the Supervision of Communications, Information Technology and Mass Communications ("**Roskomnadzor**") proposes to expand the law on personal data, following discussions held with the State Duma Committee on combatting cybercrime. In particular, the Roskomnadzor proposed to target foreign internet entities, as well as limit cross-border data transfers, with the view of protecting the rights of Russian citizens. More specifically, the Roskomnadzor emphasised that principles laid down in the field of personal data should be applied to foreign websites, which may be achieved via agreements between the Roskomnadzor and foreign authorities. (More)

Day Before Election, 6.5 Million Israel's Voters Data Leaked Online

On March 22, 2021, the Israel newspaper Haaretz repoted that a day before the Israel election, hackers post lists detailing names, ID numbers and voting location of all Israeli adults online. In the two leaked encrypted databases, one contains the full list of eligible voters, including the names and designated polling stations of 6.5 million Israelis, and the other contains over 6 million full names, ID numbers and

sometimes additional details. A massage from the hackers said they were motivated by the continuous use of Elector, a so-called campaign-management app, by political parties. (More)

Ikea France Being Prosecuted for Spying on Staff

On March 22, 2021, according to *Yahoo! Finance* report, the French branch of Swedish retailing giant Ikea went on trial, accused of running an elaborate system to spy on staff and job applicants using private detectives and police officers. Prosecutors say Ikea France collected details on hundreds of existing and prospective staff, including confidential information about criminal records, as part of a "spying system". The charges include illegally gathering personal information, receiving illegally gathered personal information, and violating professional confidentiality. Ikea France, which employs 10,000 people, faces a fine of up to 3.75 million euros. The 15 people being tried in the court include former store managers and top executives. The group also includes four police officers accused of handing over confidential information. (More)

Subscribe to our WeChat community

Beijing | Shanghai | Wuhan | Guangzhou | Shenzhen | Korea

www.lifanglaw.com
Email：info@lifanglaw.com
Tel：+8610 64096099
Fax：+8610 64096260/64096261