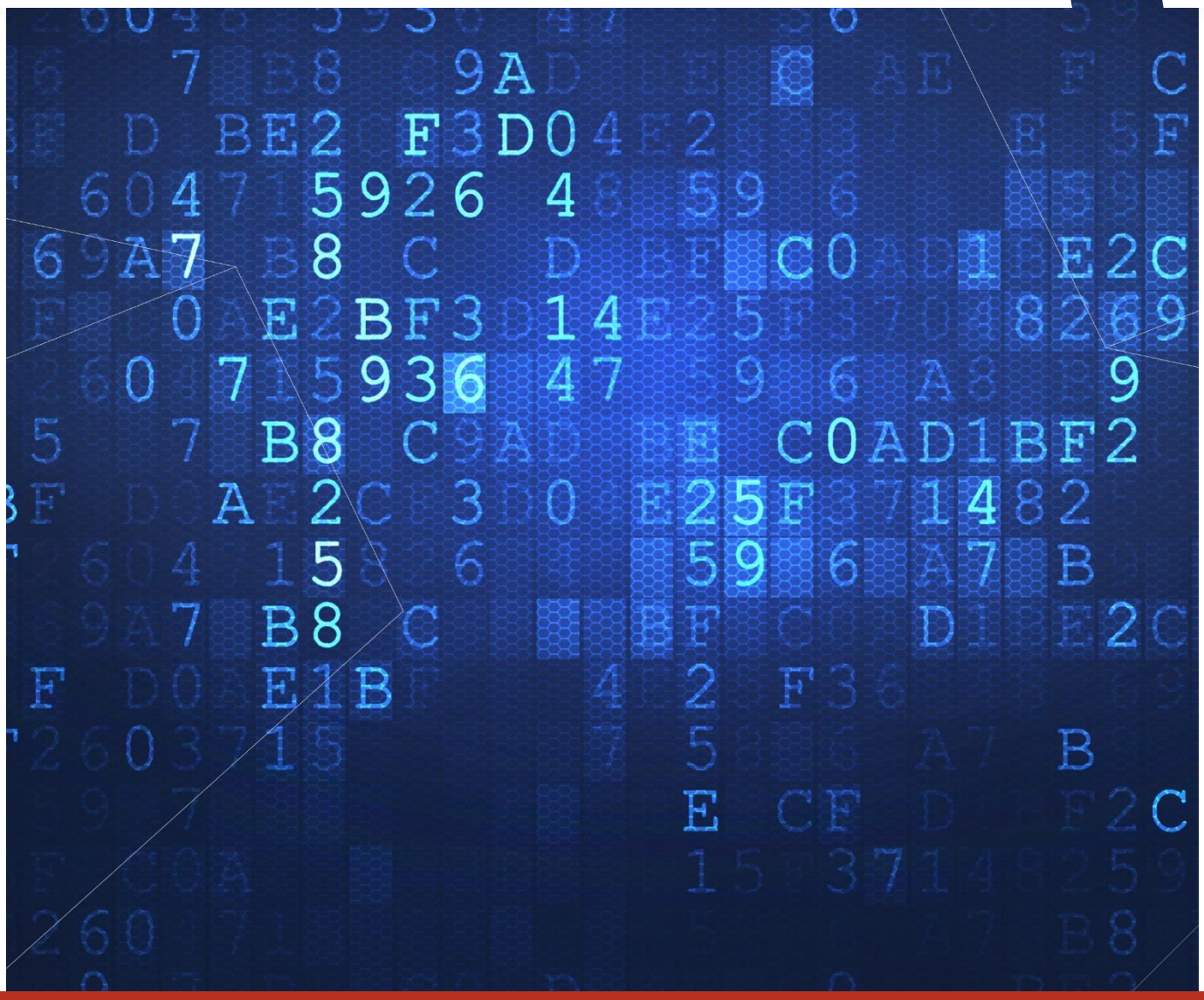
Llinks Client Alert – Cybersecurity, Data & Privacy

September 2020



Shanghai · Beijing · Shenzhen · Hong Kong · London

LINKS Law Offices
通力律师事务所

I. Legislation

Recently, the Ministry of Public Security issued *the Guidance on the Implementation of the Network Security Multi-level Protection Scheme and the Critical Information Infrastructure Security Protection Scheme* (the **"Protection Scheme Guidance"**), which provides for detailed requirements on the network security multi-level protection scheme ("**MLPS**") and the critical information infrastructure scheme. The Protection Scheme Guidance requires the network operators to complete the filing procedure and to perform the MLPS level assessment, as well as to rectify the issues identified during the assessment. The Protection Scheme Guidance also states that the determination of CII must be made in accordance with the implementing rules issued by the relevant authorities and that CII operators must strengthen the protection of CIIs and the protection of the personal information and important data contained therein.

On August 10th, 2020, the *National Information Security Standardization Technical Committee* issued the "*Information Security Technology- the Determination Method on the Boundary of the Critical Information Infrastructure (Draft)"* (the **"Determination Method"**) and the "*Information Security Technology- the Evaluation Method for the Security Protection Capability of the Critical Information Infrastructure (Draft)"* (the **"Evaluation Method"**) for public consultation. The Determination Method provides for a new approach to define the boundary of a critical information infrastructure based on the "flow of critical business information during its entire life circle" (**"CBIF"**) while the Evaluation Method provides for a base to evaluate the security protection capability of critical information infrastructure.

Llinks Comments: Recently, with the publication of the Protection Scheme Guidance, the identification and protection of "CII" has become an important topic in the network security area, again. Different from the 'three-step' methodology to identify CIIs under the *Guidance for National Cyber Security Inspection Works* issued in 2016, the Determination Method provides for a wholly new method for the definition of CIIs. Under the Determination Method, the framework basis of the "CII" is defined by the "core business" which the relevant authorities determine. Then, the operators of the core business have to recognize the networks and systems which are critical to continuous and stable operation of the core business, and define the boundary of CII according to the core business information flow. The Determination Method provides for a practicable guideline for the operators of CII to follow and forms a base for future CII protection works.

On August 11st, 2020, the *Ministry of Information and Industry* (**"MIIT"**) issued the *Guidance on the Establishment of Standardized Systems of the Data Security in the Industry of Telecoms and Internet (Draft) for public comments* (the **"Data Security Guidance"**). The Data Security Guidance provides for detailed scheme for the establishment of relevant data security standards applicable to important industrial sectors under MIIT's supervision, such as 5G, mobile internet, internet of vehicles, internet of things, industry internet, cloud computing, big data, artificial intelligent, block-chain etc.

On August 20th, 2020, State Cryptography Administration issued the *revised draft Administrative Regulation for the Commercial Encryption* (the "**Commercial Encryption Regulation"**) for public comments. The Commercial Encryption Regulation outlines the requirements for the research, manufacture, sale, services, testing, certification, import and export, application etc. of the commercial encryption. For networks or information systems such as critical information infrastructures which do not contain any state secret, the networks of which the network security level are graded level 3 or above, and the national e-government information systems, their operators are required by the Commercial Encryption Regulation to use or apply the commercial encryption to protect them.

II. Court Rulings

The High People's Court of Jiangsu Province made a final decision on an unfair competition case appealed by Aiqiyi. The decision clarifies that the court will not be too "strict" in determining the notification obligation and management obligation which the computing service providers under the"IaaS"model bear when it receives a complaint from right holders because "they are not allowed to access, control, retrieve user's data from (its client s') servers and they are subject to a relatively strict confidential obligation." Meanwhile, the court also ruled that cloud computing service providers will not be exempted from its corresponding notification obligation merely because it is a cloud computing service provider providing basic network services.

III. Law Enforcement

On August 17th, the Public Security Bureau of Sanhe City, Hebei Province found three companies which the **operate critical information infrastructures** failed to establish security training and assessment system, to perform MLPS classification obligation, or to assume network security protection responsibilities when performing network security inspections. Pursuant to Art.33, Art.34. Art.36, Art.38 and Art.59 (2) of the Cyber Security Law, the Public Security Bureau of Sanhe City imposed administrative warnings to those three companies.

In this August, several banking financial institutions have been imposed monetary penalties due to failures to protect personal data. The penalties are summarized below.

Financial Institution	Grounds of Sanction	Penalty
Credit Card Center of China Merchant Bank	Failed to protect the security of customer's personal information	A fine of RMB one million
Pacific Credit Card Center of Communication Bank	Failed to protect the security of customer's personal information	A fine of RMB one million
HSBC	Search of credit information without client's authorization	A fine of RMB 450,000
Huaibei Branch of China Bank	Search of credit information (including both individual and enterprises) without consent	A fine of RMB 370,000

On August 19th, MIIT conducted a re-examination against the app operators which were notified of being infringing users' rights and interests in MIIT's public notification issued on July 24th, 2020. Eight applications were found failing to rectify the non-compliance as required by MIIT. MITT ordered that those 8 applications be removed from application stores since August 19th.

IV. Foreign Trends

A British police force's use of facial recognition technology has been ruled unlawful in a landmark judgment at the Court of Appeal of the United Kingdom. This appeal concerns the lawfulness of the use of automated facial recognition technology (**"AFR"**) in a pilot project by the South Wales Police Force ("**SWP**"). AFR is a new technology used to assess whether two facial images depict the same person. The specific type of AFR works by extracting faces captured in a live feed from a camera and automatically comparing them to faces on a "watchlist" prepared by SWP in advance. If no match is detected, the software will automatically delete the facial image captured from the live feed. If a match is detected, the technology produces an alert and a police officer of SWP will review the images to determine whether to make an intervention. The grounds where the Court of Appeal held the SWP is unlawful includes there is no clear guidance on the selection of persons who would be put on the "watchlist", and there is no adequate "data protection impact assessment", and SWP's failure to demonstrate that the police will not use the AFR on the discriminatory grounds of races and genders etc.

About Llinks' Cyber Security and Data Compliance Services

Llinks' partners have been representing clients in data and cyber security related legal matters, such as offshore server, log records storage and filing, personal data collection and use, data integrity, centralized data process, differentiation between trade secrets and state secrets, etc. After 2010, Llinks' partners started to represent domestic and foreign enterprises in forming whole-process compliance solutions for the collection, use, transfer and destruction of customer personal information in digital marketing environment. In the course of handling these cases, Llinks' team has built up its solid capacity in tracing the logical chain which underlies all the data privacy laws and regulations. On that basis, our team can provide clients with practical and economical solutions which meet the requirements of the regulatory authorities.

Our team also includes some experienced lawyers who previously have served as law enforcement officials in cyber security administration. Their insights contribute to a better understanding on the regulatory authorities' key concerns and priorities in law enforcement, which is critically important for us to work out a practical solution for clients.

We have been working closely with relevant government consultancy departments and academic research institutions on the trend of legislation and implementation of the CSL regime. Our team has published special reports and analytical articles in this field, such as *Interpretation and Practice of the CSL*, *Practical Guidance on Trans-border Transmission Personal Information and Important Data*. In September 2018, LexisNexis published a special issue written by our team, on *Companies' Compliance in the Context of China*, which contains six articles on practical issues concerning cyber security and data compliance. In September 2018, we drafted a series of concise bilingual articles titled *30 Questions About the CSL*, which were later exclusively published online by Wolters Kluwer. Based on the latest legislation and practices, in 2019, we once again joined force with Wolters Kluwer to systematically update *30 Questions About the CSL* and publish the updated version titled *The Blue Book of PRC Cybersecurity and Data Compliance (Bilingual Version)*.

For more information, please contact:

David Pan Lawyer
Mob: +86 136 2172 0830
Tel: +86 21 3135 8701
david.pan@llinkslaw.com

Kenneth Kong Lawyer
Mob: +86 185 1210 5880
Tel: +86 21 3135 8777
kenneth.kong@llinkslaw.com

Xun Yang
Mob: +86 152 2182 2373
Tel: +86 21 3135 8799
xun.yang@llinkslaw.com

Patrick Gu Lawyer
Mob: +86 188 1746 8818
Tel: +86 21 3135 8722
patrick.gu@llinkslaw.com

Nigel Zhu Lawyer

Jianqi Yang Lawyer

Susan Deng